No. 20-1191

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

WIKIMEDIA FOUNDATION,

Plaintiff–Appellant,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants–Appellees.

On Appeal from the United States District Court
for the District of Maryland at Baltimore

JOINT APPENDIX—VOLUME 1 OF 7 (JA0001–JA0919)

H. Thomas Byron III
Joseph Busa
Michael Shih
U.S. DEPARTMENT OF JUSTICE
950 Pennsylvania Ave. NW
Washington, DC 20530
Phone: (202) 616-5367
Fax: (202) 307-2551
h.thomas.byron@usdoj.gov

Counsel for Defendants–Appellees

Patrick Toomey
Ashley Gorski
Charles Hogle
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
ptoomey@aclu.org

Counsel for Plaintiff–Appellant
(Additional counsel on next page)

Alex Abdo
Jameel Jaffer
KNIGHT FIRST AMENDMENT INSTITUTE AT COLUMBIA UNIVERSITY
475 Riverside Drive, Suite 302
New York, NY 10115
Phone: (646) 745-8500
alex.abdo@knightcolumbia.org

Deborah A. Jeon
David R. Rocah
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND
3600 Clipper Mill Rd., #350
Baltimore, MD 21211
Phone: (410) 889-8555
Fax: (410) 366-7838
rocah@aclu-md.org

Benjamin H. Kleine
COOLEY LLP
101 California Street, 5th Floor
San Francisco, CA 94111
Phone: (415) 693-2000
Fax: (415) 693-2222
bkleine@cooley.com

***Wikimedia Foundation v. National Security Agency, et al.*,**
No. 20-1191 (4th Cir.)

JOINT APPENDIX
Table of Contents

VOLUME 1

Exhibits to Wikimedia Foundation's Motion to Compel

Exhibits to Defendants' Opposition to Wikimedia Foundation's Motion to Compel

Exhibits to Wikimedia Foundation's Reply in Support of Its Motion to Compel

Opinion & Order Denying Wikimedia Foundation's Motion to Compel

Exhibits to Defendants' Motion for Summary Judgment

VOLUME 2

Exhibits to Wikimedia Foundation's Opposition to Defendants' Motion for Summary Judgment

VOLUME 3

Exhibits to Wikimedia Foundation's Opposition to Defendants' Motion for Summary Judgment (Cont'd)

VOLUME 4

Exhibits to Wikimedia Foundation's Opposition to Defendants' Motion for Summary Judgment (Cont'd)

VOLUME 5

Exhibits to Wikimedia Foundation's Opposition to Defendants' Motion for Summary Judgment (Cont'd)

VOLUME 6

Exhibits to Defendants' Reply in Support of Their Motion for Summary Judgment

VOLUME 7

Exhibits to Wikimedia Foundation's Sur-reply in Opposition to Defendants' Motion for Summary Judgment

Exhibits to Defendants' Sur-reply in Support of Their Motion for Summary Judgment

Opinion & Order Granting Defendants' Motion for Summary Judgment

Wikimedia Foundation's Notice of Appeal

APPEAL,CLOSED

U.S. District Court
District of Maryland (Baltimore)
CIVIL DOCKET FOR CASE #: 1:15-cv-00662-TSE

Wikimedia Foundation et al v. National Security Agency/Central Security Service et al
Assigned to: Judge T. NA S. Ellis
Case in other court: USCA, 15-02560
US Court of Appeals for the 4th Circuit, 20-01191
Cause: 05:706 Judicial Review of Agency Action

Date Filed: 03/10/2015
Date Terminated: 10/23/2015
Jury Demand: None
Nature of Suit: 440 Civil Rights: Other
Jurisdiction: U.S. Government Defendant

Plaintiff

Wikimedia Foundation represented by **Alex Abdo**
Knight First Amendment Institute at Columbia University
475 Riverside Dr. Ste. 302
New York, NY 10115
6467458500
Email: alex.abdo@knightcolumbia.org
PRO HAC VICE
ATTORNEY TO BE NOTICED

Ashley Marie Gorski
American Civil Liberties Union Foundation
125 Broad St
18th Floor
New York, NY 10004
2122847305
Fax: 2125492654
Email: agorski@aclu.org
PRO HAC VICE
ATTORNEY TO BE NOTICED

Benjamin Hansel Kleine
Cooley LLP
101 California St. 5th Floor
San Francisco, CA 94111
4156932000
Fax: 4156932222
Email: bkleine@cooley.com
PRO HAC VICE
ATTORNEY TO BE NOTICED

Charles Sims
Proskauer Rose LLP
11 Times Square
New York, NY 10036
2129693950

Fax: 2129692900
Email: csims@proskauer.com
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Alexander Munkittrick
Proskauer Rose LLP
11 Times Square
New York, NY 10036
2129693226
Fax: 2129692900
Email: dmunkittrick@proskauer.com
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Robert Rocah
ACLU of Maryland
3600 Clipper Mill Rd, #350
Baltimore, MD 21211
14108898555
Fax: 14103667838
Email: rocah@aclu-md.org
ATTORNEY TO BE NOTICED

Devon Cook
Cooley LLP
101 California St. 5th Floor
San Francisco, CA 94111
4156932000
Fax: 4156932222
Email: dhanleycook@cooley.com
PRO HAC VICE
ATTORNEY TO BE NOTICED

Jameel Jaffer
Knight First Amendment Institute at
Columbia University
475 Riverside Drive
Suite 302
New York, NY 10115
6467458500
Email: jameel.jaffer@knightcolumbia.org
PRO HAC VICE
ATTORNEY TO BE NOTICED

John Browning
Proskauer Rose LLP
11 Times Square
New York, NY 10036
2129693452
Fax: 2129692900
Email: jbrowning@proskauer.com
PRO HAC VICE
ATTORNEY TO BE NOTICED

Jonathan Hafetz
American Civil Liberties Union Foundation
125 Broad St. 18th Fl.
New York, NY 10004
2122847319
Fax: 2125492517
Email: jhafetz@aclu.org
PRO HAC VICE
ATTORNEY TO BE NOTICED

Molly Smolen
Cooley LLP
101 California St. 5th Floor
San Francisco, CA 94111
4156932000
Fax: 4156932222
Email: msmolen@cooley.com
PRO HAC VICE
ATTORNEY TO BE NOTICED

Patrick Toomey
American Civil Liberties Union Foundation
125 Broad St
18th Floor
New York, NY 10004
2125197816
Fax: 2125492654
Email: ptoomey@aclu.org
PRO HAC VICE
ATTORNEY TO BE NOTICED

Deborah A Jeon
American Civil Liberties Union of Maryland Foundation
3600 Clipper Mill Rd Ste 350
Baltimore, MD 21211
14108898555
Fax: 14103667838
Email: jeon@aclu-md.org
ATTORNEY TO BE NOTICED

Plaintiff

National Association of Criminal Defense Attorneys

represented by

Alex Abdo
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Ashley Marie Gorski
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Charles Sims

(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Alexander Munkittrick
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Robert Rocah
(See above for address)
ATTORNEY TO BE NOTICED

Jameel Jaffer
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

John Browning
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Jonathan Hafetz
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Patrick Toomey
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Deborah A Jeon
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Human Rights Watch represented by **Alex Abdo**
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Ashley Marie Gorski
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Charles Sims
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Alexander Munkittrick

(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Robert Rocah
(See above for address)
ATTORNEY TO BE NOTICED

Jameel Jaffer
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

John Browning
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Jonathan Hafetz
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Patrick Toomey
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Deborah A Jeon
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Pen American Center represented by **Alex Abdo**
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Ashley Marie Gorski
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Charles Sims
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Alexander Munkittrick
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Robert Rocah

(See above for address)
ATTORNEY TO BE NOTICED

Jameel Jaffer
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

John Browning
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Jonathan Hafetz
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Patrick Toomey
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Deborah A Jeon
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Global Fund for Women represented by **Alex Abdo**
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Ashley Marie Gorski
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Charles Sims
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Alexander Munkittrick
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Robert Rocah
(See above for address)
ATTORNEY TO BE NOTICED

Jameel Jaffer
(See above for address)

PRO HAC VICE
ATTORNEY TO BE NOTICED

John Browning
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Jonathan Hafetz
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Patrick Toomey
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Deborah A Jeon
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

The Nation Magazine represented by **Alex Abdo**
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Ashley Marie Gorski
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Charles Sims
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Alexander Munkittrick
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Robert Rocah
(See above for address)
ATTORNEY TO BE NOTICED

Jameel Jaffer
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

John Browning
(See above for address)

PRO HAC VICE
ATTORNEY TO BE NOTICED

Jonathan Hafetz
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Patrick Toomey
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Deborah A Jeon
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

The Rutherford Institute represented by **Alex Abdo**
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Ashley Marie Gorski
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Charles Sims
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Alexander Munkittrick
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Robert Rocah
(See above for address)
ATTORNEY TO BE NOTICED

Jameel Jaffer
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

John Browning
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Jonathan Hafetz
(See above for address)

PRO HAC VICE
ATTORNEY TO BE NOTICED

Patrick Toomey
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Deborah A Jeon
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Washington Office on Latin America represented by **Alex Abdo**
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Ashley Marie Gorski
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Charles Sims
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Alexander Munkittrick
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Robert Rocah
(See above for address)
ATTORNEY TO BE NOTICED

Jameel Jaffer
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

John Browning
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Jonathan Hafetz
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Patrick Toomey
(See above for address)

PRO HAC VICE
ATTORNEY TO BE NOTICED

Deborah A Jeon
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Amnesty International USA represented by **Alex Abdo**
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Ashley Marie Gorski
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Charles Sims
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Alexander Munkittrick
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Robert Rocah
(See above for address)
ATTORNEY TO BE NOTICED

Jameel Jaffer
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

John Browning
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Jonathan Hafetz
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Patrick Toomey
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Deborah A Jeon

(See above for address)
ATTORNEY TO BE NOTICED

V.

Defendant

National Security Agency/Central Security Service

represented by **James Jordan Gilligan**
United States Department of Justice
Civil Division, Federal Programs Branch
1100 L Street, N.W.
Room 11200
Washington, DC 20005
2025143358
Fax: 2026168470
Email: james.gilligan@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Julia Alexandra Berman
United States Department of Justice
Civil Division Federal Programs Branch
1100 L Street, NW
Washington, DC 20005
2026168480
Fax: 2026168470
Email: julia.heiman@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Olivia R. Hussey Scott
USDOJ Civil Division
1100 L Street, N.W.
Room 11112
Washington, DC 20005
2026168491
Fax: 2026168470
Email: Olivia.Hussey.Scott@usdoj.gov
ATTORNEY TO BE NOTICED

Rodney Patton
United States Department of Justice
20 Massachusetts Ave
Rm 7320
Washington, DC 20530
2023057919
Fax: 2026168470
Email: rodney.patton@usdoj.gov
ATTORNEY TO BE NOTICED

Timothy A Johnson
Dept. of Justice
20 Massachusetts Ave NW
Washington, DC 20530

2025141359
Fax: 2026168470
Email: timothy.johnson4@usdoj.gov

Defendant

Adm. Michael S. Rogers
in his official capacity as Director of the National Security Agency and Chief of the Central Security Service

represented by **James Jordan Gilligan**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Julia Alexandra Berman
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Olivia R. Hussey Scott
(See above for address)
ATTORNEY TO BE NOTICED

Rodney Patton
(See above for address)
ATTORNEY TO BE NOTICED

Timothy A Johnson
(See above for address)

Defendant

Office of the Director of National Intelligence

represented by **James Jordan Gilligan**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Julia Alexandra Berman
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Olivia R. Hussey Scott
(See above for address)
ATTORNEY TO BE NOTICED

Rodney Patton
(See above for address)
ATTORNEY TO BE NOTICED

Timothy A Johnson
(See above for address)

Defendant

James R. Clapper
in his official capacity as Director of National Intelligence

represented by **James Jordan Gilligan**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Julia Alexandra Berman
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Olivia R. Hussey Scott
(See above for address)
ATTORNEY TO BE NOTICED

Rodney Patton
(See above for address)
ATTORNEY TO BE NOTICED

Timothy A Johnson
(See above for address)

Defendant

Department of Justice represented by **James Jordan Gilligan**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Julia Alexandra Berman
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Olivia R. Hussey Scott
(See above for address)
ATTORNEY TO BE NOTICED

Rodney Patton
(See above for address)
ATTORNEY TO BE NOTICED

Timothy A Johnson
(See above for address)

Defendant

Eric H. Holder represented by **James Jordan Gilligan**
in his official capacity as Attorney General of the United States
TERMINATED: 06/22/2015
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Julia Alexandra Berman
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Olivia R. Hussey Scott
(See above for address)
ATTORNEY TO BE NOTICED

Rodney Patton
(See above for address)
ATTORNEY TO BE NOTICED

Defendant

Loretta E. Lynch
in her official capacity as Attorney General of the United States

represented by **James Jordan Gilligan**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Julia Alexandra Berman
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Olivia R. Hussey Scott
(See above for address)
ATTORNEY TO BE NOTICED

Rodney Patton
(See above for address)
ATTORNEY TO BE NOTICED

Timothy A Johnson
(See above for address)

Amicus

CloudFlare
CloudFlare

represented by **Jeffrey Landis**
ZwillGen PLLC
1900 M Street, NW
Suite 250
Washington, DC 20036
12027065203
Fax: 12027065298
Email: jeff@zwillgen.com

Jennifer Stisa Granick
Stanford Center for Internet and Society
559 Nathan Abbot Way
Stanford, CA 94305
6507368675
Email: jennifer@law.stanford.edu
PRO HAC VICE
ATTORNEY TO BE NOTICED

Amicus

The Tor Project, Inc.
The Tor Project, Inc.

represented by **Jeffrey Landis**
(See above for address)

Jennifer Stisa Granick
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Amicus

RiseUp
RiseUp

represented by **Jeffrey Landis**
(See above for address)

Jennifer Stisa Granick
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Amicus

First Amendment Legal Scholars

represented by **Emily Lange Levenson**
Brown, Goldstein & Levy LLP
120 E. Baltimore St
Suite 1700
Baltimore, MD 21202
4109621030
Fax: 4103850869
Email: elevenson@browngold.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joshua R Treem
Brown Goldstein Levy LLP
120 E Baltimore St Ste 1700
Baltimore, MD 21202
14109621030
Fax: 14103850869
Email: jtreem@browngold.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Margot E Kaminski
Moritz College of Law, The Ohio State University
55 W 12th Ave
Columbus, OH 43210
6142922092
Email: kaminski.217@osu.edu
PRO HAC VICE
ATTORNEY TO BE NOTICED

Amicus

The American Booksellers Association

represented by **Andrew Gellis Crocker**
Electronic Frontier Foundation
815 Eddy St
San Franscisco, CA 94109
4154369333
Fax: 4154369993
Email: andrew@eff.org
PRO HAC VICE
ATTORNEY TO BE NOTICED

Jan Ingham Berlage

Gohn Hankey & Berlage, LLP
201 N Charles St Ste 2101
Baltimore, MD 21201
14107529300
Fax: 14107522519
Email: jberlage@ghsllp.com
ATTORNEY TO BE NOTICED

Amicus

American Library Association represented by **Andrew Gellis Crocker**
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Jan Ingham Berlage
(See above for address)
ATTORNEY TO BE NOTICED

Amicus

Association of Research Libraries represented by **Andrew Gellis Crocker**
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Jan Ingham Berlage
(See above for address)
ATTORNEY TO BE NOTICED

Amicus

Freedom to Read Foundation represented by **Andrew Gellis Crocker**
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Jan Ingham Berlage
(See above for address)
ATTORNEY TO BE NOTICED

Amicus

International Federation of Library Associations and Institutions represented by **Andrew Gellis Crocker**
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Jan Ingham Berlage
(See above for address)
ATTORNEY TO BE NOTICED

Date Filed	#	Docket Text
03/10/2015	1	COMPLAINT *for Declaratory and Injunctive Relief* against All Defendants (Filing fee $ 400 receipt number 0416-5260730.), filed by The Nation Magazine, Human Rights Watch, The Rutherford Institute, National Association of Criminal Defense Attorneys,

		Washington Office on Latin America, Pen American Center, Wikimedia Foundation, Global Fund for Women, Amnesty International USA. (Attachments: # 1 Civil Cover Sheet, # 2 Summonses)(Jeon, Deborah) (Entered: 03/10/2015)
03/10/2015	2	NOTICE by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation *Summons to U.S. Attorney* (Jeon, Deborah) (Entered: 03/10/2015)
03/10/2015	3	Summons Issued 60 days as to James R. Clapper, Department of Justice, Eric H. Holder, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers, U.S. Attorney and U.S. Attorney General (bmhs, Deputy Clerk) (Entered: 03/10/2015)
03/10/2015	4	MOTION to Appear Pro Hac Vice for Alex Abdo (Filing fee $ 50, receipt number 0416-5262165.) by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation (Rocah, David) (Entered: 03/10/2015)
03/10/2015	5	MOTION to Appear Pro Hac Vice for Ashley Gorski (Filing fee $ 50, receipt number 0416-5262203.) by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation (Rocah, David) (Entered: 03/10/2015)
03/10/2015	6	MOTION to Appear Pro Hac Vice for Jameel Jaffer (Filing fee $ 50, receipt number 0416-5262236.) by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation (Rocah, David) (Entered: 03/10/2015)
03/10/2015	7	MOTION to Appear Pro Hac Vice for Patrick Toomey (Filing fee $ 50, receipt number 0416-5262246.) by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation (Rocah, David) (Entered: 03/10/2015)
03/10/2015	8	QC NOTICE: 4 Motion to Appear Pro Hac Vice, filed by Wikimedia Foundation, Pen American Center, The Nation Magazine, National Association of Criminal Defense Attorneys, Global Fund for Women, Human Rights Watch, Washington Office on Latin America, The Rutherford Institute, Amnesty International USA needs to be modified. See attachment for details and corrective actions needed regarding the signature(s) on the motion. (bu, Deputy Clerk) (Entered: 03/10/2015)
03/10/2015	9	QC NOTICE: 5 Motion to Appear Pro Hac Vice, filed by Wikimedia Foundation, Pen American Center, The Nation Magazine, National Association of Criminal Defense Attorneys, Global Fund for Women, Human Rights Watch, Washington Office on Latin America, The Rutherford Institute, Amnesty International USA needs to be modified. See attachment for details and corrective actions needed regarding the signature(s) on the motion. (bu, Deputy Clerk) (Entered: 03/10/2015)
03/10/2015	10	QC NOTICE: 6 Motion to Appear Pro Hac Vice, filed by Wikimedia Foundation, Pen American Center, The Nation Magazine, National Association of Criminal Defense Attorneys, Global Fund for Women, Human Rights Watch, Washington Office on Latin America, The Rutherford Institute, Amnesty International USA needs to be modified. See

		attachment for details and corrective actions needed regarding the signature(s) on the motion. (bu, Deputy Clerk) (Entered: 03/10/2015)
03/10/2015	11	QC NOTICE: 7 Motion to Appear Pro Hac Vice, filed by Wikimedia Foundation, Pen American Center, The Nation Magazine, National Association of Criminal Defense Attorneys, Global Fund for Women, Human Rights Watch, Washington Office on Latin America, The Rutherford Institute, Amnesty International USA needs to be modified. See attachment for details and corrective actions needed regarding the signature(s) on the motion. (bu, Deputy Clerk) (Entered: 03/10/2015)
03/11/2015	12	CORRECTED MOTION to Appear Pro Hac Vice for Alex Abdo by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation (Attachments: # 1 Signature page). The fee has already been paid.(Rocah, David) (Entered: 03/11/2015)
03/11/2015	13	CORRECTED MOTION to Appear Pro Hac Vice for Ashley Gorski by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation (Attachments: # 1 Signature page). The fee has already been paid.(Rocah, David) (Entered: 03/11/2015)
03/11/2015	14	PAPERLESS ORDER granting 12 Corrected Motion to Appear Pro Hac Vice on behalf of Alex Abdo. Directing attorney Alex Abdo to register online for CM/ECF at https://www.mdd.uscourts.gov/attyregB/inputProHac.asp. Signed by Clerk on 3/11/2015. (bu, Deputy Clerk) (Entered: 03/11/2015)
03/11/2015	15	PAPERLESS ORDER granting 13 Corrected Motion to Appear Pro Hac Vice on behalf of Ashley Gorski. Directing attorney Ashley Gorski to register online for CM/ECF at https://www.mdd.uscourts.gov/attyregB/inputProHac.asp. Signed by Clerk on 3/11/2015. (bu, Deputy Clerk) (Entered: 03/11/2015)
03/11/2015	16	CORRECTED MOTION to Appear Pro Hac Vice for Jameel Jaffer by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation (Attachments: # 1 Signature page). The fee has already been paid.(Rocah, David) (Entered: 03/11/2015)
03/11/2015	17	CORRECTED MOTION to Appear Pro Hac Vice for Patrick Toomey by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation (Attachments: # 1 Signature page). The fee has already been paid.(Rocah, David) (Entered: 03/11/2015)
03/11/2015	18	MOTION to Appear Pro Hac Vice for Charles Sims (Filing fee $ 50, receipt number 0416-5265356.) by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation (Attachments: # 1 Signature page)(Rocah, David) (Entered: 03/11/2015)
03/11/2015	19	MOTION to Appear Pro Hac Vice for David Munkittrick (Filing fee $ 50, receipt number 0416-5265372.) by Amnesty International USA, Global Fund for Women,

		Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation (Attachments: # 1 Signature page)(Rocah, David) (Entered: 03/11/2015)
03/11/2015	20	MOTION to Appear Pro Hac Vice for John Browning (Filing fee $ 50, receipt number 0416-5265384.) by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation (Attachments: # 1 Signature page)(Rocah, David) (Entered: 03/11/2015)
03/11/2015	21	PAPERLESS ORDER granting 16 Corrected Motion to Appear Pro Hac Vice on behalf of Jameel Jaffer. Directing attorney Jameel Jaffer to register online for CM/ECF at https://www.mdd.uscourts.gov/attyregB/inputProHac.asp. Signed by Clerk on 3/11/2015. (bu, Deputy Clerk) (Entered: 03/11/2015)
03/11/2015	22	PAPERLESS ORDER granting 17 Corrected Motion to Appear Pro Hac Vice on behalf of Patrick Toomey. Directing attorney Patrick Toomey to register online for CM/ECF at https://www.mdd.uscourts.gov/attyregB/inputProHac.asp. Signed by Clerk on 3/11/2015. (bu, Deputy Clerk) (Entered: 03/11/2015)
03/11/2015	23	PAPERLESS ORDER granting 18 Motion to Appear Pro Hac Vice on behalf of Charles Sims. Directing attorney Charles Sims to register online for CM/ECF at https://www.mdd.uscourts.gov/attyregB/inputProHac.asp. Signed by Clerk on 3/11/2015. (bu, Deputy Clerk) (Entered: 03/11/2015)
03/11/2015	24	PAPERLESS ORDER granting 19 Motion to Appear Pro Hac Vice on behalf of David Munkittrick. Directing attorney David Munkittrick to register online for CM/ECF at https://www.mdd.uscourts.gov/attyregB/inputProHac.asp. Signed by Clerk on 3/11/2015. (bu, Deputy Clerk) (Entered: 03/11/2015)
03/11/2015	25	PAPERLESS ORDER granting 20 Motion to Appear Pro Hac Vice on behalf of John Browning. Directing attorney John Browning to register online for CM/ECF at https://www.mdd.uscourts.gov/attyregB/inputProHac.asp. Signed by Clerk on 3/11/2015. (bu, Deputy Clerk) (Entered: 03/11/2015)
03/11/2015	26	Local Rule 103.3 Disclosure Statement by Amnesty International USA. (Rocah, David) (Entered: 03/11/2015)
03/11/2015	27	Local Rule 103.3 Disclosure Statement by Global Fund for Women. (Rocah, David) (Entered: 03/11/2015)
03/11/2015	28	Local Rule 103.3 Disclosure Statement by Human Rights Watch. (Rocah, David) (Entered: 03/11/2015)
03/11/2015	29	Local Rule 103.3 Disclosure Statement by National Association of Criminal Defense Attorneys identifying Other Affiliate Foundation for Criminal Justice for National Association of Criminal Defense Attorneys.. (Rocah, David) (Entered: 03/11/2015)
03/11/2015	30	Local Rule 103.3 Disclosure Statement by Pen American Center. (Rocah, David) (Entered: 03/11/2015)
03/11/2015	31	Local Rule 103.3 Disclosure Statement by The Rutherford Institute. (Rocah, David) (Entered: 03/11/2015)
03/11/2015	32	Local Rule 103.3 Disclosure Statement by The Nation Magazine. (Rocah, David) (Entered: 03/11/2015)

03/11/2015	33	Local Rule 103.3 Disclosure Statement by Wikimedia Foundation. (Rocah, David) (Entered: 03/11/2015)
03/11/2015	34	Local Rule 103.3 Disclosure Statement by Washington Office on Latin America. (Rocah, David) (Entered: 03/11/2015)
03/17/2015	35	(FILED IN ERROR) AFFIDAVIT of Service for Summons served on United States Attorney for the District of Maryland on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) Modified on 3/17/2015 (bmhs, Deputy Clerk). (Entered: 03/17/2015)
03/17/2015	36	(FILED IN ERROR) AFFIDAVIT of Service for Summons served on Office of the Director of National Intelligence on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) Modified on 3/17/2015 (bmhs, Deputy Clerk). (Entered: 03/17/2015)
03/17/2015	37	(FILED IN ERROR) AFFIDAVIT of Service for Summons served on National Security Agency / Central Security Service on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) Modified on 3/17/2015 (bmhs, Deputy Clerk). (Entered: 03/17/2015)
03/17/2015	38	(FILED IN ERROR) AFFIDAVIT of Service for Summons served on Department of Justice on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) Modified on 3/17/2015 (bmhs, Deputy Clerk). (Entered: 03/17/2015)
03/17/2015	39	(FILED IN ERROR) AFFIDAVIT of Service for Summons served on Adm. Michael S. Rogers on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) Modified on 3/17/2015 (bmhs, Deputy Clerk). (Entered: 03/17/2015)
03/17/2015	40	(FILED IN ERROR) AFFIDAVIT of Service for Summons served on Director of National Intelligence James R. Clapper on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) Modified on 3/17/2015 (bmhs, Deputy Clerk). (Entered: 03/17/2015)
03/17/2015	41	(FILED IN ERROR) AFFIDAVIT of Service for Summons served on Attorney General Eric H. Holder, Jr. on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) Modified on 3/17/2015 (bmhs, Deputy Clerk). (Entered: 03/17/2015)
03/17/2015	42	QC NOTICE: 35 Affidavit of Service filed by Wikimedia Foundation, Pen American Center, The Nation Magazine, National Association of Criminal Defense Attorneys,

		Global Fund for Women, Human Rights Watch, Washington Office on Latin America, The Rutherford Institute, Amnesty International USA was filed incorrectly. ***Incorrect event was selected. Please refile using the event under Service of Process - Summons Returned Executed as to USA AND case caption and case number are missing. It has been noted as FILED IN ERROR, and the document link has been disabled.* (bmhs, Deputy Clerk) (Entered: 03/17/2015)
03/17/2015	43	QC NOTICE: 36 37 38 39 40 41 Affidavits of Service filed by Wikimedia Foundation, Pen American Center, The Nation Magazine, National Association of Criminal Defense Attorneys, Global Fund for Women, Human Rights Watch, Washington Office on Latin America, The Rutherford Institute, Amnesty International USA were filed incorrectly. ***Case caption and case number are missing. It has been noted as FILED IN ERROR, and the document link has been disabled.* (bmhs, Deputy Clerk) (Entered: 03/17/2015)
03/17/2015	44	SUMMONS Returned Executed by The Nation Magazine, Amnesty International USA, Human Rights Watch, The Rutherford Institute, National Association of Criminal Defense Attorneys, Washington Office on Latin America, Wikimedia Foundation, Pen American Center, Global Fund for Women. James R. Clapper served on 3/10/2015, answer due 5/11/2015; Department of Justice served on 3/10/2015, answer due 5/11/2015; Eric H. Holder served on 3/10/2015, answer due 5/11/2015; National Security Agency/Central Security Service served on 3/10/2015, answer due 5/11/2015; Office of the Director of National Intelligence served on 3/10/2015, answer due 5/11/2015; Michael S. Rogers served on 3/10/2015, answer due 5/11/2015. (Toomey, Patrick) (Entered: 03/17/2015)
03/17/2015	45	AFFIDAVIT of Service for Summons served on Office of the Director of National Intelligence on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) (Entered: 03/17/2015)
03/17/2015	46	AFFIDAVIT of Service for Summons served on National Security Agency / Central Security Service on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) (Entered: 03/17/2015)
03/17/2015	47	AFFIDAVIT of Service for Summons served on Director of National Intelligence James R. Clapper on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) (Entered: 03/17/2015)
03/17/2015	48	AFFIDAVIT of Service for Summons served on Department of Justice on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) (Entered: 03/17/2015)
03/17/2015	49	AFFIDAVIT of Service for Summons served on Adm. Michael S. Rogers on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) (Entered: 03/17/2015)
03/17/2015	50	AFFIDAVIT of Service for Summons served on Attorney General Eric H. Holder, Jr. on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights

		Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) (Entered: 03/17/2015)
03/19/2015	51	NOTICE of Appearance by James Jordan Gilligan on behalf of All Defendants (Gilligan, James) (Entered: 03/19/2015)
03/23/2015	52	NOTICE of Appearance by Rodney Patton on behalf of James R. Clapper, Department of Justice, Eric H. Holder, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers (Patton, Rodney) (Entered: 03/23/2015)
03/24/2015	53	NOTICE of Appearance by Julia Alexandra Berman on behalf of All Defendants (Berman, Julia) (Entered: 03/24/2015)
03/26/2015		Case reassigned to Judge T. S. Ellis. Judge Richard D Bennett no longer assigned to the case. (cags, Deputy Clerk) (Entered: 03/26/2015)
04/24/2015	54	MOTION to Set a Status Conference by James R. Clapper, Department of Justice, Eric H. Holder, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers Responses due by 5/11/2015 (Attachments: # 1 Exhibit 1, # 2 Text of Proposed Order)(Berman, Julia) (Entered: 04/24/2015)
04/28/2015	55	RESPONSE to Motion re 54 MOTION to Set a Status Conference filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. Replies due by 5/15/2015. (Attachments: # 1 Text of Proposed Order)(Toomey, Patrick) (Entered: 04/28/2015)
04/30/2015	56	ORDER granting 54 Defendants' Motion to set a status conference; and scheduling a status conference for 3:30 p.m. on Wednesday, May 13, 2015. Signed by Judge T. S. Ellis on 4/30/2015. (bmhs, Deputy Clerk) (Entered: 04/30/2015)
05/06/2015	57	Correspondence re: Request Pursuant to D. Md. Local Rule 101.1(b)(i) for May 13, 2015 Status Conference (Toomey, Patrick) (Entered: 05/06/2015)
05/11/2015	58	ORDER granting 57 Plaintiffs' Letter Motion. Signed by Judge T. S. Ellis on 5/11/15. (bmhs, Deputy Clerk) (Entered: 05/11/2015)
05/12/2015	59	PAPERLESS ORDER, for good cause, it is hereby ORDERED that the status conference scheduled to be heard at the Greenbelt Courthouse at 3:30 p.m. on Wednesday, May 13, 2015, is CANCELED. Instead, a telephone conference is SCHEDULED for the same date and time (3:30 p.m. on Wednesday, May 13, 2015). In this regard, all participating counsel are DIRECTED first to conference themselves together on one phone line and then to call Chambers at (703) 299-2114 to commence the conference call. Signed by Judge T. S. Ellis on 5/12/2015. (bmhs, Deputy Clerk) (Entered: 05/12/2015)
05/14/2015	60	Telephone Conference held on 5/14/2015 before Judge T. S. Ellis. (bmhs, Deputy Clerk) (Entered: 05/15/2015)
05/14/2015	61	ORDER directing parties to comply with the briefing and argument schedule. Signed by Judge T. S. Ellis on 5/13/2015. (bmhs, Deputy Clerk) (Entered: 05/15/2015)
05/27/2015	62	MOTION to Set a Date for the Filing of Amicus Briefs by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation Responses due by

		6/15/2015 (Attachments: # 1 Text of Proposed Order)(Toomey, Patrick) (Entered: 05/27/2015)
05/28/2015	63	ORDER denying 62 Motion to Set a Date for the Filing of Amicus Briefs. Signed by Judge T. S. Ellis on 5/28/2015. (bmhs, Deputy Clerk) (Entered: 05/28/2015)
05/29/2015	64	Joint MOTION to Conduct Hearings in Alexandria, Virginia by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation Responses due by 6/15/2015 (Attachments: # 1 Text of Proposed Order)(Toomey, Patrick) (Entered: 05/29/2015)
05/29/2015	65	ORDER granting 64 Joint Motion to Conduct Hearings in Alexandria, Virginia. Signed by Judge T. S. Ellis on 5/29/2015. (bmhs, Deputy Clerk) (Entered: 05/29/2015)
05/29/2015	66	MOTION to Dismiss for Lack of Jurisdiction *Under Rule 12(b)(1)* by James R. Clapper, Department of Justice, Eric H. Holder, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers Responses due by 6/15/2015 (Attachments: # 1 Memorandum of Law in Support of Motion to Dismiss, # 2 Text of Proposed Order, # 3 Exhibit Exhibit List, # 4 Exhibit Exhibit 1, # 5 Exhibit Exhibit 2, # 6 Exhibit Exhibit 3, # 7 Exhibit Exhibit 4A, # 8 Exhibit Exhibit 4B, # 9 Exhibit Exhibit 4C, # 10 Exhibit Exhibit 4D, # 11 Exhibit Exhibit 5, # 12 Exhibit Exhibit 6)(Patton, Rodney) (Entered: 05/29/2015)
06/12/2015	67	Joint MOTION to Amend the Briefing Schedule by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation Responses due by 6/29/2015 (Attachments: # 1 Text of Proposed Order)(Toomey, Patrick) (Entered: 06/12/2015)
06/12/2015	68	ORDER granting 67 Joint Motion to Amend the Briefing Scheduling governing Defendants' Motion to Dismiss; and postponing the oral argument on Defendants' Motion to Dismiss. Signed by Judge T. S. Ellis on 6/12/2015. (bmhs, Deputy Clerk) (Entered: 06/15/2015)
06/12/2015	69	ORDER amending the briefing schedule. Signed by Judge T. S. Ellis on 6/12/2015. (bmhs, Deputy Clerk) (Entered: 06/15/2015)
06/19/2015	70	MOTION to Amend/Correct 1 Complaint, by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation Responses due by 7/9/2015 (Attachments: # 1 First Amended Complaint, # 2 First Amended Complaint - Redline, # 3 Text of Proposed Order)(Toomey, Patrick) (Entered: 06/19/2015)
06/22/2015	71	ORDER granting 70 Plaintiffs' Motion to Amend the Complaint; and denying as moot 66 Defendants' Motion to Dismiss. Signed by Judge T. S. Ellis on 6/22/2015. (bmhs, Deputy Clerk) (Entered: 06/22/2015)
06/22/2015	72	AMENDED COMPLAINT against James R. Clapper, Department of Justice, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers, Loretta E. Lynch filed by The Nation Magazine, Amnesty International USA, Human Rights Watch, The Rutherford Institute, National Association of Criminal Defense Attorneys, Washington Office on Latin America, Wikimedia Foundation, Pen American Center, Global Fund for Women. (Attachments: # 1 Red Line Complaint)(bmhs, Deputy Clerk) (Entered: 06/22/2015)

06/27/2015	73	Consent MOTION for Extension of Time by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers Responses due by 7/16/2015 (Attachments: # 1 Text of Proposed Order)(Berman, Julia) (Entered: 06/27/2015)
06/29/2015	74	ORDER granting 73 Consent Motion for Extension of Time. Signed by Judge T. S. Ellis on 6/29/2015. (bmhs, Deputy Clerk) (Entered: 06/29/2015)
07/31/2015	75	MOTION to Appear Pro Hac Vice for Jennifer Stisa Granick (Filing fee $ 50, receipt number 0416-5525629.) by CloudFlare, The Tor Project, Inc., RiseUp (Landis, Jeffrey) (Entered: 07/31/2015)
08/03/2015	76	PAPERLESS ORDER granting 75 Motion to Appear Pro Hac Vice on behalf of Jennifer Stisa Granick. Directing attorney Jennifer Stisa Granick to register online for CM/ECF at https://www.mdd.uscourts.gov/attyregB/inputProHac.asp. Signed by Clerk on 8/3/2015. (bu, Deputy Clerk) (Entered: 08/03/2015)
08/06/2015	77	MOTION to Dismiss for Lack of Jurisdiction by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers Responses due by 8/24/2015 (Attachments: # 1 (Memorandum in Support), # 2 Affidavit (Salzberg Declaration), # 3 Affidavit (Lee Declaration Part 1), # 4 Affidavit (Lee Declaration Part 2), # 5 Affidavit (Lee Declaration Part 3), # 6 Affidavit (Lee Declaration Part 4), # 7 Affidavit (Lee Declaration Part 5), # 8 Exhibit 1, # 9 Exhibit 2, # 10 Exhibit 3, # 11 Exhibit 4, # 12 Exhibit 5, # 13 Exhibit 6, # 14 Exhibit 7, # 15 Exhibit 8, # 16 Exhibit 9, # 17 (Index of Exhibits), # 18 Text of Proposed Order)(Gilligan, James) (Entered: 08/06/2015)
09/03/2015	78	NOTICE of Appearance by Joshua R Treem on behalf of First Amendment Legal Scholars (Treem, Joshua) (Entered: 09/03/2015)
09/03/2015	79	NOTICE of Appearance by Emily Lange Levenson on behalf of First Amendment Legal Scholars (Levenson, Emily) (Entered: 09/03/2015)
09/03/2015	80	MOTION to Appear Pro Hac Vice (Filing fee $ 50, receipt number 0416-5581832.) by First Amendment Legal Scholars (Treem, Joshua) (Entered: 09/03/2015)
09/03/2015	81	NOTICE of Appearance by Jan Ingham Berlage on behalf of The American Booksellers Association, American Library Association, Association of Research Libraries, Freedom to Read Foundation, International Federation of Library Associations and Institutions (Berlage, Jan) (Entered: 09/03/2015)
09/03/2015	82	MOTION for Leave to File *to File Brief of Amici Curiae in Support of Plaintiffs' Opposition to Defendants' Motion to Dismiss* by American Library Association, Association of Research Libraries, Freedom to Read Foundation, International Federation of Library Associations and Institutions, The American Booksellers Association Responses due by 9/21/2015 (Attachments: # 1 Brief in Opposition to Defendants' Motion to Dismiss)(Berlage, Jan) (Entered: 09/03/2015)
09/03/2015	83	MOTION to Appear Pro Hac Vice for Andrew Crocker (Filing fee $ 50, receipt number 0416-5582368.) by American Library Association, Association of Research Libraries, Freedom to Read Foundation, International Federation of Library Associations and Institutions, The American Booksellers Association (Berlage, Jan) (Entered: 09/03/2015)
09/03/2015	84	NOTICE by American Library Association, Association of Research Libraries, Freedom to Read Foundation, International Federation of Library Associations and Institutions, The American Booksellers Association re 81 Notice of Appearance, 82 MOTION for Leave to File *to File Brief of Amici Curiae in Support of Plaintiffs' Opposition to Defendants' Motion to Dismiss*, 83 MOTION to Appear Pro Hac Vice for Andrew

		Crocker (Filing fee $ 50, receipt number 0416-5582368.) *of Service* (Berlage, Jan) (Entered: 09/03/2015)
09/03/2015	85	MOTION for Leave to File *Brief of Amicus Curiae* by First Amendment Legal Scholars Responses due by 9/21/2015 (Attachments: # 1 Brief of Amicus Curiae First Amendment Legal Scholars, # 2 Text of Proposed Order)(Treem, Joshua) (Entered: 09/03/2015)
09/03/2015	86	RESPONSE in Opposition re 77 MOTION to Dismiss for Lack of Jurisdiction filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. Replies due by 9/21/2015. (Toomey, Patrick) (Entered: 09/03/2015)
09/09/2015	87	PAPERLESS ORDER granting 80 Motion to Appear Pro Hac Vice on behalf of Margot E Kaminski. Directing attorney Margot E Kaminski to register online for CM/ECF at https://www.mdd.uscourts.gov/attyregB/inputProHac.asp. Signed by Clerk on 9/9/2015. (srd, Intern) (Entered: 09/09/2015)
09/09/2015	88	PAPERLESS ORDER granting 83 Motion to Appear Pro Hac Vice on behalf of Andrew Crocker. Directing attorney Andrew Crocker to register online for CM/ECF at https://www.mdd.uscourts.gov/attyregB/inputProHac.asp. Signed by Clerk on 9/9/2015. (srd, Intern) (Entered: 09/09/2015)
09/17/2015	89	REPLY to Response to Motion re 77 MOTION to Dismiss for Lack of Jurisdiction filed by James R. Clapper, Department of Justice, Eric H. Holder, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers. (Attachments: # 1 Exhibit 1)(Gilligan, James) (Entered: 09/17/2015)
09/25/2015	90	Status Conference held on 9/25/2015 before Judge T. S. Ellis. (Court Reporter: M. Pham) (bmhs, Deputy Clerk) (Entered: 09/28/2015)
09/25/2015	91	ORDER taking under advisment 77 Defendant's MOTION to Dismiss for Lack of Jurisdiction. Signed by Judge T. S. Ellis on 9/25/2015. (bmhs, Deputy Clerk) (Entered: 09/28/2015)
10/22/2015	92	MOTION to Withdraw as Attorney by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation Responses due by 11/9/2015 (Attachments: # 1 Text of Proposed Order)(Rocah, David) (Entered: 10/22/2015)
10/23/2015	93	MEMORANDUM OPINION. Signed by Judge T. S. Ellis on 10/23/2015. (bmhs, Deputy Clerk) (Entered: 10/23/2015)
10/23/2015	94	ORDER granting 82 85 amici curiae's Motions for Leave to File amicus curiae briefs. Signed by Judge T. S. Ellis on 10/23/2015. (bmhs, Deputy Clerk) (Entered: 10/23/2015)
10/23/2015	95	ORDER granting 77 Defendants' Motion to Dismiss. Signed by Judge T. S. Ellis on 10/23/2015. (bmhs, Deputy Clerk) (Entered: 10/23/2015)
12/15/2015	96	NOTICE OF APPEAL as to 95 Order on Motion to Dismiss/Lack of Jurisdiction by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. Filing fee $ 505, receipt number 0416-5759619. (Toomey, Patrick) (Entered: 12/15/2015)
12/17/2015	97	Transmission of Notice of Appeal and Docket Sheet to US Court of Appeals re 96 Notice of Appeal. IMPORTANT NOTICE: To access forms which you are required to file with the United States Court of Appeals for the Fourth Circuit please go to

		http://www.ca4.uscourts.gov and click on Forms & Notices. (sls, Deputy Clerk) (Entered: 12/17/2015)
12/18/2015	98	USCA Case Number 15-2560 for 96 Notice of Appeal, filed by Wikimedia Foundation, Pen American Center, The Nation Magazine, National Association of Criminal Defense Attorneys, Global Fund for Women, Human Rights Watch, Washington Office on Latin America, The Rutherford Institute, Amnesty International USA. Case Manager - RJ Warren (ko, Deputy Clerk) (Entered: 12/18/2015)
12/29/2015	99	(ELECTRONICALLY FILED IN ERROR)TRANSCRIPT REQUEST by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation for proceedings held on September 25, 2015 before Judge T.S. Ellis, III.. (Toomey, Patrick) Modified on 12/29/2015 (slss, Deputy Clerk). (Entered: 12/29/2015)
01/04/2016	100	NOTICE OF FILING OF OFFICIAL TRANSCRIPT for dates of September 25, 2015, before Judge T.S. Ellis, III, re 96 Notice of Appeal, Court Reporter/Transcriber Michael A. Rodriquez, Telephone number 301-213-4913. Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date it may be obtained from the Court Reporter or through PACER. Does this satisfy all appellate orders for this reporter? - Y. Redaction Request due 1/25/2016. Redacted Transcript Deadline set for 2/4/2016. Release of Transcript Restriction set for 4/4/2016. (jbps, Deputy Clerk) (Entered: 01/04/2016)
05/23/2017	101	JUDGMENT of USCA (certified copy) affirming in part and vacating in part the judgment of the district court; remanding the case to the district court for further proceedings consistent with the court's decision as to 96 Notice of Appeal, filed by Wikimedia Foundation, Pen American Center, The Nation Magazine, National Association of Criminal Defense Attorneys, Global Fund for Women, Human Rights Watch, Washington Office on Latin America, The Rutherford Institute, Amnesty International USA (kr2, Deputy Clerk) (Entered: 05/23/2017)
07/17/2017	102	MANDATE of USCA issued as to 96 Notice of Appeal, filed by Wikimedia Foundation, Pen American Center, The Nation Magazine, National Association of Criminal Defense Attorneys, Global Fund for Women, Human Rights Watch, Washington Office on Latin America, The Rutherford Institute, Amnesty International USA (ko, Deputy Clerk) (Entered: 07/17/2017)
07/17/2017	103	MOTION for a Status Conference by Wikimedia Foundation (Attachments: # 1 Text of Proposed Order)(Toomey, Patrick) (Entered: 07/17/2017)
07/31/2017	104	RESPONSE to Motion re 103 MOTION for a Status Conference filed by National Security Agency/Central Security Service, Office of the Director of National Intelligence. (Attachments: # 1 Text of Proposed Order)(Berman, Julia) (Entered: 07/31/2017)
08/02/2017	105	ORDER granting 103 Motion for a Status Conference and Briefing Schedule; directing Plaintiff to submit a brief; and scheduling a hearing. Signed by Judge T. S. Ellis on 8/2/2017. (bmhs, Deputy Clerk) (Entered: 08/02/2017)
08/03/2017	106	MOTION to Appear Pro Hac Vice for Jonathan Hafetz (Filing fee $100, receipt number 0416-6813625.) by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation(Rocah, David) (Entered: 08/03/2017)
08/11/2017	107	RESPONSE re 105 Order on Motion for Miscellaneous Relief filed by Wikimedia

		Foundation.(Toomey, Patrick) (Entered: 08/11/2017)
08/15/2017	108	PAPERLESS ORDER granting 106 Motion to Appear Pro Hac Vice on behalf of Jonathan Hafetz. Directing attorney Jonathan Hafetz to register online for CM/ECF at http://www.mdd.uscourts.gov/electronic-case-filing-registration. Signed by Clerk on 8/15/2017. (srd, Deputy Clerk) (Entered: 08/15/2017)
08/26/2017	109	RESPONSE re 107 Response *(Defendants' Response to Plaintiff's Brief Regarding How This Matter Should Proceed)* filed by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers.(Gilligan, James) (Entered: 08/26/2017)
08/28/2017	110	Consent MOTION for Extension of Time *(Unopposed Motion For An Eight-Hour Extension Of Time Nunc Pro Tunc To File Defendants Response To Plaintiffs Brief Regarding How This Matter Should Proceed)* by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers (Attachments: # 1 Text of Proposed Order)(Gilligan, James) (Entered: 08/28/2017)
09/01/2017	111	RESPONSE re 109 Response, filed by Wikimedia Foundation.(Toomey, Patrick) (Entered: 09/01/2017)
09/06/2017	112	PAPERLESS ORDER rescheduling the status conference from September 8, 2017 to September 22, 2017 at 1:00 p.m. Signed by Judge T. S. Ellis on 9/6/2017. (bmhs, Deputy Clerk) (Entered: 09/06/2017)
09/13/2017	113	NOTICE of Appearance by Timothy A Johnson on behalf of All Defendants (Johnson, Timothy) (Entered: 09/13/2017)
09/22/2017	115	Status Conference held on 9/22/2017 before Judge T. S. Ellis.(Court Reporter: Michael A. Rodriquez) (bmhs, Deputy Clerk) (Entered: 09/28/2017)
09/27/2017	114	ORDER directing parties to file a joint status plan for discovery on jurisdictional issues. Signed by Judge T. S. Ellis on 9/25/2017. (bmhs, Deputy Clerk) (Entered: 09/27/2017)
09/28/2017	116	REPORT of Rule 26(f) Planning Meeting (Attachments: # 1 Text of Proposed Order) (Patton, Rodney) (Entered: 09/28/2017)
10/03/2017	117	ORDER granting parties 5 months of discovery to commence on 10/17/17. Signed by Judge T. S. Ellis on 10/3/2017. (bmhs, Deputy Clerk) (Entered: 10/05/2017)
10/16/2017	118	ANSWER to 72 Amended Complaint,, by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers.(Gilligan, James) (Entered: 10/16/2017)
12/28/2017	119	NOTICE by Wikimedia Foundation *of Stipulated Protective Order* (Gorski, Ashley) (Entered: 12/28/2017)
12/29/2017	120	STIPULATED PROTECTIVE ORDER Approving terms and conditions of parties re: confidential information. Signed by Judge T. S. Ellis on 12/29/2017 (cags, Deputy Clerk) (Entered: 12/29/2017)
01/12/2018	121	NOTICE OF FILING OF OFFICIAL TRANSCRIPT of Proceedings held on 9/22/17, before Judge T.S. Ellis, III. Court Reporter/Transcriber Tonia M. Harris. Total number of pages filed: 50. Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date it may be obtained from the Court Reporter or through PACER. Redaction Request due 2/2/2018. Redacted Transcript Deadline set for

		2/12/2018. Release of Transcript Restriction set for 4/12/2018.(bmhs, Deputy Clerk) (Entered: 01/12/2018)
03/12/2018	122	Joint MOTION for Other Relief *(Joint Motion to Continue Discovery Deadline Pending Parties Submission of a Proposed Schedule for Completion of Jurisdictional Discovery)* by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers (Attachments: # 1 Text of Proposed Order)(Gilligan, James) (Entered: 03/12/2018)
03/15/2018	123	ORDER denying 122 Joint Motion to Continue Discovery Deadline Pending Parties Submission of a Proposed Schedule for Completion of Jurisdictional Discovery. Signed by Judge T. S. Ellis on 3/15/2018. (bmhs, Deputy Clerk) (Entered: 03/16/2018)
03/22/2018	124	Joint MOTION for Other Relief *(Joint Motion to Set Briefing Schedule for Motions to Compel)* by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers (Attachments: # 1 Text of Proposed Order, # 2 Exhibit A - Memorandum from Attorney General)(Johnson, Timothy) (Entered: 03/22/2018)
03/26/2018	125	Local Rule 104.7 Certificate (Attachments: # 1 Motion to Compel Discovery Responses and Deposition Testimony, # 2 Memorandum in Support of Motion to Compel, # 3 Affidavit Declaration of Patrick Toomey, # 4 Exhibit 1, # 5 Exhibit 2, # 6 Exhibit 3, # 7 Exhibit 4, # 8 Exhibit 5, # 9 Exhibit 6, # 10 Exhibit 7, # 11 Exhibit 8, # 12 Exhibit 9, # 13 Exhibit 10, # 14 Exhibit 11, # 15 Exhibit 12, # 16 Exhibit 13, # 17 Exhibit 14, # 18 Exhibit 15, # 19 Exhibit 16, # 20 Exhibit 17, # 21 Exhibit 18, # 22 Exhibit 19, # 23 Exhibit 20, # 24 Exhibit 21, # 25 Exhibit 22, # 26 Exhibit 23, # 27 Exhibit 24, # 28 Exhibit 25, # 29 Exhibit 26, # 30 Exhibit 27, # 31 Exhibit 28, # 32 Exhibit 29, # 33 Exhibit 30, # 34 Text of Proposed Order)(Toomey, Patrick) (Entered: 03/26/2018)
03/26/2018	126	MOTION to Compel *Discovery* by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers (Attachments: # 1 Exhibit (Memorandum in Support), # 2 Exhibit (Exhibit 1), # 3 Exhibit (Exhibit 2), # 4 Errata (Exhibit 3), # 5 Text of Proposed Order)(Gilligan, James) (Entered: 03/26/2018)
03/28/2018	127	NOTICE of Appearance by Olivia R. Hussey Scott on behalf of All Defendants (Scott, Olivia) (Entered: 03/28/2018)
04/06/2018	128	MOTION to Appear Pro Hac Vice for Molly A. Smolen (Filing fee $100, receipt number 0416-7257344.) by Wikimedia Foundation(Rocah, David) (Entered: 04/06/2018)
04/06/2018	129	MOTION to Appear Pro Hac Vice for Benjamin H. Kleine (Filing fee $100, receipt number 0416-7257347.) by Wikimedia Foundation(Rocah, David) (Entered: 04/06/2018)
04/06/2018	130	MOTION to Appear Pro Hac Vice for Devon Hanley Cook (Filing fee $100, receipt number 0416-7257349.) by Wikimedia Foundation(Rocah, David) (Entered: 04/06/2018)
04/06/2018	132	ORDER re: 124 parties' Joint Motion to Set Briefing Schedule for Motions to Compel. Signed by Judge T. S. Ellis on 4/6/2018. (bmhs, Deputy Clerk) (Entered: 04/09/2018)
04/07/2018	131	NOTICE by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers re 126 MOTION to Compel *Discovery (Notice of Withdrawal of Motion to Compel)* (Gilligan, James) (Entered: 04/07/2018)
04/10/2018	133	PAPERLESS ORDER granting 128 Motion to Appear Pro Hac Vice on behalf of Molly Smolen. Directing attorney Molly Smolen to register online for CM/ECF at

		http://www.mdd.uscourts.gov/electronic-case-filing-registration. Signed by Clerk on 4/10/2018. (srd, Deputy Clerk) (Entered: 04/10/2018)
04/10/2018	134	PAPERLESS ORDER granting 129 Motion to Appear Pro Hac Vice on behalf of Benjamin Kleine. Directing attorney Benjamin Kleine to register online for CM/ECF at http://www.mdd.uscourts.gov/electronic-case-filing-registration. Signed by Clerk on 4/10/2018. (srd, Deputy Clerk) (Entered: 04/10/2018)
04/10/2018	135	PAPERLESS ORDER granting 130 Motion to Appear Pro Hac Vice on behalf of Devon Cook. Directing attorney Devon Cook to register online for CM/ECF at http://www.mdd.uscourts.gov/electronic-case-filing-registration. Signed by Clerk on 4/10/2018. (srd, Deputy Clerk) (Entered: 04/10/2018)
04/18/2018	136	Supplemental to 125 Local Rule,,, filed by Wikimedia Foundation *Supplement to Plaintiff's Motion to Compel 125* (Toomey, Patrick) (Entered: 04/18/2018)
04/27/2018	137	NOTICE by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers (Patton, Rodney) (Entered: 04/27/2018)
04/28/2018	138	RESPONSE re 125 Local Rule,,, *in Opposition to Plaintiff's Motion to Compel Discovery Responses and Deposition Testimony* filed by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers. (Attachments: # 1 Exhibit A, # 2 Exhibit B, # 3 Exhibit C, # 4 Exhibit D, # 5 Text of Proposed Order)(Gilligan, James) (Entered: 04/28/2018)
04/28/2018	139	MOTION for Extension of Time to File *Out of Time* by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers (Attachments: # 1 Text of Proposed Order)(Gilligan, James) (Entered: 04/28/2018)
04/30/2018	140	ORDER granting 139 Defendants' Out-of-Time Motion for a Five and One-Half Hour Extension of Time. Signed by Judge T. S. Ellis on 4/30/2018. (bmhs, Deputy Clerk) Modified on 5/1/2018 (bmhs, Deputy Clerk). (Entered: 05/01/2018)
05/11/2018	141	NOTICE by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers *(Notice of Filing Unclassified (Redacted) Version of Classified Declaration Lodged With the Court In Camera and Ex Parte on April 27, 2018, in Support of the Government's Assertion of the State Secrets Privilege and Related Statutory Privileges)* (Attachments: # 1 Exhibit (Redacted Declaration of George C. Barnes, Deputy Director, National Security Agency))(Gilligan, James) (Entered: 05/11/2018)
05/17/2018	142	RESPONSE re 132 Order on Motion for Other Relief . *Joint Response to Court Order re: June 1, 2018 Hearing* filed by Wikimedia Foundation.(Toomey, Patrick) (Entered: 05/17/2018)
05/18/2018	143	RESPONSE re 138 Response, *Reply Brief in Support of Plaintiff's Motion to Compel* filed by Wikimedia Foundation. (Attachments: # 1 Declaration of Ashley Gorski, # 2 Exhibit 1, # 3 Exhibit 2)(Gorski, Ashley) (Entered: 05/18/2018)
05/29/2018	144	ORDER rescheduling the upcoming hearing on Plaintiff's Motion to Compel. Signed by Judge T. S. Ellis on 5/29/2018. (bmhs, Deputy Clerk) (Entered: 05/29/2018)
06/08/2018	145	Consent MOTION to Withdraw as Attorney *(Timothy A. Johnson)* by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security

		Service, Office of the Director of National Intelligence, Michael S. Rogers(Johnson, Timothy) (Entered: 06/08/2018)
06/22/2018	146	ORDER granting 145 Motion to Withdraw as Attorney. Attorney Timothy A Johnson terminated. Signed by Judge T. S. Ellis on 6/21/2018. (bmhs, Deputy Clerk) (Entered: 06/22/2018)
06/28/2018	147	Correspondence Correcting Earlier Submission: 138 Response, (Attachments: # 1 Attachment Corrected Version of Defendants' Memorandum of Points and Authorities in Opposition to Plaintiff's Motion to Compel Discovery Responses and Deposition Testimony)(Scott, Olivia) (Entered: 06/28/2018)
07/06/2018	148	Supplemental to 125 Local Rule,,, filed by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers *(Defendants' Supplemental Memorandum in Opposition to Plaintiffs' Motion to Compel)* (Gilligan, James) (Entered: 07/06/2018)
07/06/2018	149	Supplemental to 125 Local Rule,,, filed by Wikimedia Foundation *(Plaintiff's Supplemental Brief in Response to the Court's June 29, 2018 Order)* (Gorski, Ashley) (Entered: 07/06/2018)
08/20/2018	150	MEMORANDUM OPINION. Signed by Judge T. S. Ellis on 8/20/2018. (bmhs, Deputy Clerk) (Entered: 08/20/2018)
08/20/2018	151	ORDER denying 126 Plaintiff's Motion to Compel Discovery Responses and Deposition Testimony. Signed by Judge T. S. Ellis on 8/20/2018. (bmhs, Deputy Clerk) (Entered: 08/20/2018)
08/31/2018	152	ORDER scheduling a status conference. Signed by Judge T. S. Ellis on 8/31/2018. (bmhs, Deputy Clerk) (Entered: 09/04/2018)
09/04/2018	153	ORDER scheduling a status conference. Signed by Judge T. S. Ellis on 9/4/2018. (bmhs, Deputy Clerk) (Entered: 09/04/2018)
09/18/2018	154	MOTION for Other Relief *(Motion to Set a Summary Judgment Briefing Schedule)* by Wikimedia Foundation (Attachments: # 1 Text of Proposed Order)(Toomey, Patrick) (Entered: 09/18/2018)
09/20/2018	155	MOTION to Set a Summary Judgment Briefing Schedule and Response to Plaintiff's Motion to Set a Summary Judgment Briefing Schedule re 154 MOTION for Other Relief *(Motion to Set a Summary Judgment Briefing Schedule)* by James R. Clapper, Department of Justice, Eric H. Holder, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers (Attachments: # 1 Text of Proposed Order)(Scott, Olivia) (Entered: 09/20/2018)
09/21/2018	156	ORDER granting in part and denying in part 154 Plaintiff's Motion to Set a Summary Judgment Briefing Schedule; and granting in part and denying in part 155 Defendants' Motion to Set a Summary Judgment Briefing Schedule. Signed by Judge T. S. Ellis on 9/21/2018. (bmhs, Deputy Clerk) (Entered: 09/24/2018)
09/21/2018	157	Status Conference held on 9/21/2018 before Judge T. S. Ellis.(Court Reporter: Tonia Harris) (bmhs, Deputy Clerk) (Entered: 09/26/2018)
09/26/2018	158	ORDER setting briefing and oral argument schedule. Signed by Judge T. S. Ellis on 9/25/2018. (bmhs, Deputy Clerk) (Entered: 09/26/2018)
11/06/2018	159	MOTION for Extension of Time to File *MSJ - Unopposed Motion for Extension of One*

		Business Day to Submit Defendants Summary Judgment Motion by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers (Attachments: # 1 Text of Proposed Order)(Berman, Julia) (Entered: 11/06/2018)
11/13/2018	160	MOTION for Extension of Time to File *Motion for Summary Judgment; Defendants Out-of-Time Motion for Extension of One Business Day to Submit Defendants Summary Judgment Motion* by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers (Attachments: # 1 Text of Proposed Order)(Berman, Julia) (Entered: 11/13/2018)
11/13/2018	161	MOTION for Summary Judgment by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers (Attachments: # 1 Text of Proposed Order, # 2 Memorandum in Support (Filed Under Seal), # 3 Exhibit List (Filed Under Seal), # 4 Exhibit 1 (Filed Under Seal), # 5 Exhibit 2 (Filed Under Seal), # 6 Exhibit 3 (Filed Under Seal), # 7 Exhibit 4 (Filed Under Seal), # 8 Exhibit 5 (Filed Under Seal))(Gilligan, James) (Entered: 11/13/2018)
11/13/2018	162	-SEALED - NOTICE of Filing Under Seal Sealed Brief in Support of Defendants' Motion for Summary Judgment and Sealed Exhibits by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers re 161 MOTION for Summary Judgment (Attachments: # 1 Sealed Exhibit List, # 2 Sealed Exhibit 1, # 3 Sealed Exhibit 2, # 4 Sealed Exhibit 3, # 5 Sealed Exhibit 4, # 6 Sealed Exhibit 5)(Gilligan, James) (Entered: 11/13/2018)
11/13/2018	163	MOTION to Seal *Defendants' Summary Judgment Motion Pursuant to Civil Local Rule 105-11 and Protective Order Paragraph 12.3* by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers (Attachments: # 1 Text of Proposed Order)(Gilligan, James) (Entered: 11/13/2018)
12/07/2018	164	MOTION for Leave to File *Updated Public Versions of the Under Seal Portions of Defendants' Motion for Summary Judgment* by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers (Attachments: # 1 Text of Proposed Order, # 2 Attachment A, # 3 Attachment B, # 4 Attachment C, # 5 Attachment D, # 6 Attachment E, # 7 Attachment F, # 8 Attachment G)(Scott, Olivia) (Entered: 12/07/2018)
12/11/2018	165	ORDER granting 163 Defendants' Motion to Seal; and granting 164 Defendants' Motion for Leave to File an Updated Public Version of Defendants' Sealed Motion for Summary Judgment. Signed by Judge T. NA S. Ellis on 12/11/2018. (bmhs, Deputy Clerk) (Entered: 12/11/2018)
12/11/2018	166	Supplemental Exhibits A-G to 161 Motion for Summary Judgment. (Attachments: # 1 Exhibit B, # 2 Exhibit C, # 3 Exhibit D, # 4 Exhibit E, # 5 Exhibit F, # 6 Exhibit G) (bmhs, Deputy Clerk) (Entered: 12/11/2018)
12/18/2018	167	MOTION for Extension of Time to File *Opposition to Motion for Summary Judgment; Plaintiff's Out-of-Time Motion for Extension to Submit Opposition to Defendants' Summary Judgment Motion* by Wikimedia Foundation (Attachments: # 1 Text of Proposed Order)(Toomey, Patrick) (Entered: 12/18/2018)
12/18/2018	168	RESPONSE in Opposition re 161 MOTION for Summary Judgment filed by Wikimedia Foundation. (Attachments: # 1 Exhibit List, # 2 Exhibit 1 - Declaration of Scott Bradner,

		# 3 Exhibit 1 - Appendix to Bradner Declaration [1/3], # 4 Exhibit 1 - Appendix to Bradner Declaration [2/3], # 5 Exhibit 1 - Appendix to Bradner Declaration [3/3], # 6 Exhibit 2 - Declaration of Jonathon Penney, # 7 Exhibit 3 - Declaration of Michelle Paulson, # 8 Exhibit 4 - Declaration of James Alexander, # 9 Exhibit 5 - Declaration of Tilman Bayer, # 10 Exhibit 6 - Declaration of Emily Temple-Wood, # 11 Exhibit 7 - Declaration of Patrick Toomey, # 12 Exhibit 8, # 13 Exhibit 9, # 14 Exhibit 10, # 15 Exhibit 11, # 16 Exhibit 12, # 17 Exhibit 13, # 18 Exhibit 14, # 19 Exhibit 15, # 20 Exhibit 16, # 21 Exhibit 17, # 22 Exhibit 18, # 23 Exhibit 19, # 24 Exhibit 20, # 25 Exhibit 21, # 26 Exhibit 22, # 27 Exhibit 23, # 28 Exhibit 24, # 29 Exhibit 25, # 30 Exhibit 26, # 31 Exhibit 27, # 32 Exhibit 28, # 33 Exhibit 29, # 34 Exhibit 30, # 35 Exhibit 31, # 36 Exhibit 32, # 37 Exhibit 33, # 38 Exhibit 34, # 39 Exhibit 35, # 40 Exhibit 36, # 41 Exhibit 37, # 42 Exhibit 38, # 43 Exhibit 39, # 44 Exhibit 40, # 45 Exhibit 41, # 46 Exhibit 42, # 47 Exhibit 43, # 48 Exhibit 44, # 49 Exhibit 45, # 50 Text of Proposed Order)(Toomey, Patrick) (Entered: 12/18/2018)
12/19/2018	169	ORDER granting 167 Plaintiff's Out-of-Time Motion for an Extension of Time to File Its Opposition to Defendants' Motion for Summary Judgment. Signed by Judge T. NA S. Ellis on 12/19/2018. (bmhs, Deputy Clerk) (Entered: 12/19/2018)
12/19/2018	170	ORDER granting 159 Defendants' Out-of-Time Motion for Extension of One Business Day to Submit Defendants' Summary Judgment Motion. Signed by Judge T. NA S. Ellis on 12/19/2018. (bmhs, Deputy Clerk) (Entered: 12/19/2018)
12/26/2018	171	MOTION to Stay *of Proceedings in Light of Lapse of Appropriations* by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers (Attachments: # 1 Text of Proposed Order)(Scott, Olivia) (Entered: 12/26/2018)
12/27/2018	172	RESPONSE re 171 MOTION to Stay *of Proceedings in Light of Lapse of Appropriations* filed by Wikimedia Foundation.(Gorski, Ashley) (Entered: 12/27/2018)
01/02/2019	173	ORDER granting 171 Motion to Stay; and vacating the 9/25/18 order establishing a briefing and oral argument schedule. Signed by Judge T. NA S. Ellis on 1/2/2019. (bmhs, Deputy Clerk) (Entered: 01/02/2019)
01/28/2019	174	NOTICE by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers *to the Court of Restoration of Appropriations* (Scott, Olivia) (Entered: 01/28/2019)
01/31/2019	175	Joint MOTION for Other Relief *(Joint Motion to Set Revised Schedule)* by Wikimedia Foundation (Attachments: # 1 Text of Proposed Order)(Gorski, Ashley) (Entered: 01/31/2019)
01/31/2019	176	ORDER LIFTING STAY. Signed by Judge T. NA S. Ellis on 1/31/2019. (kw2s, Deputy Clerk) (Entered: 01/31/2019)
02/04/2019	177	ORDER granting 175 Joint Motion to Set a Revised Schedule. Signed by Judge T. NA S. Ellis on 2/1/2019. (bmhs, Deputy Clerk) (Entered: 02/04/2019)
02/15/2019	178	REPLY to Response to Motion re 161 MOTION for Summary Judgment *(Reply Brief in Support of Defendants' Motion for Summary Judgment)* filed by James R. Clapper, Department of Justice, Eric H. Holder, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers. (Attachments: # 1 Exhibit List, # 2 Affidavit (Exh. 6 (Second) Schulzrinne Declaration), # 3 Affidavit (Exh. 7 Salzberg Declaration), # 4 Affidavit (Exh. 8 (Second) Gilligan Declaration), # 5 Exhibit 9, # 6 Exhibit 10, # 7 Exhibit 11, # 8 Exhibit 12, # 9 Exhibit 13, # 10 Exhibit 14, # 11 Exhibit 15)(Gilligan, James) (Entered: 02/15/2019)

03/01/2019	179	MOTION for Leave to File Excess Pages *[Unopposed]* by Wikimedia Foundation (Attachments: # 1 Text of Proposed Order)(Gorski, Ashley) (Entered: 03/01/2019)
03/04/2019	180	ORDER granting 179 Unopposed Motion for Leave to File Excess Pages. Signed by Judge T. NA S. Ellis on 3/4/2019. (bmhs, Deputy Clerk) (Entered: 03/04/2019)
03/08/2019	181	RESPONSE in Opposition re 161 MOTION for Summary Judgment *(Sur-reply Brief in Opposition to Defendants' Motion for Summary Judgment)* filed by Wikimedia Foundation. (Attachments: # 1 Exhibit 1. Second Bradner Declaration, # 2 Exhibit 2. Second Penney Declaration, # 3 Exhibit 3. Second Paulson Declaration, # 4 Exhibit 4. Second Bayer Declaration, # 5 Exhibit 5. Second Temple-Wood Declaration)(Toomey, Patrick) (Entered: 03/08/2019)
03/22/2019	182	REPLY to Response to Motion re 161 MOTION for Summary Judgment *(Sur-Reply in Support of Defendants' Motion for Summary Judgment)* filed by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers. (Attachments: # 1 Exhibit List, # 2 Affidavit (Exh. 16 (Third) Schulzrinne Declaration), # 3 Affidavit (Exh. 17 Second Salzberg Declaration))(Gilligan, James) (Entered: 03/22/2019)
04/03/2019	183	ORDER Rescheduling Oral Argument for May, 30 2019 at 2:00 p.m.. Signed by Judge T. NA S. Ellis on 4/3/2019. (bas, Deputy Clerk) (Entered: 04/04/2019)
04/29/2019	184	NOTICE by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers *of Recent Decision* (Attachments: # 1 Attachment)(Scott, Olivia) (Entered: 04/29/2019)
05/03/2019	185	RESPONSE re 184 Notice (Other), filed by Wikimedia Foundation.(Toomey, Patrick) (Entered: 05/03/2019)
05/30/2019	186	Civil Motion Hearing held on 5/30/2019 before Judge T. NA S. Ellis. (bmhs, Deputy Clerk) (Entered: 05/31/2019)
08/09/2019	187	(FILED IN ERROR) NOTICE OF FILING OF OFFICIAL TRANSCRIPT of Proceedings held on 5/30/2019, before Judge T.S. Ellis, III. Court Reporter/Transcriber Tonia M. Harris, Telephone number 703-646-1438. Total number of pages filed: 69. Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date it may be obtained from the Court Reporter or through PACER. Redaction Request due 8/30/2019. Redacted Transcript Deadline set for 9/9/2019. Release of Transcript Restriction set for 11/7/2019.(bmhs, Deputy Clerk) Modified on 5/12/2020 (bmhs, Deputy Clerk). (Entered: 08/09/2019)
12/16/2019	188	MEMORANDUM OPINION. Signed by Judge T. NA S. Ellis on 12/13/2019. (kw2s, Deputy Clerk) (Entered: 12/16/2019)
12/16/2019	189	ORDER Granting 161 MOTION for Summary Judgment filed by National Security Agency/Central Security Service, Loretta E. Lynch, Michael S. Rogers, Office of the Director of National Intelligence, James R. Clapper, Department of Justice. Signed by Judge T.S. Ellis on 12/13/2019. (kw2s, Deputy Clerk) Modified on 12/17/2019 (kw2s, Deputy Clerk). (Entered: 12/16/2019)
12/17/2019	190	JUDGMENT in favor of Defendants against Plaintiff. Signed by Felicia C. Cannon, Clerk of Court on 12/16/2019. (bmhs, Deputy Clerk) (Entered: 12/17/2019)
02/14/2020	191	NOTICE OF APPEAL as to 190 Clerk's Judgment by Wikimedia Foundation. Filing fee $ 505, receipt number 0416-8516425.(Toomey, Patrick) (Entered: 02/14/2020)

02/19/2020	192	Transmission of Notice of Appeal and Docket Sheet to US Court of Appeals re 191 Notice of Appeal. IMPORTANT NOTICE: To access forms which you are required to file with the United States Court of Appeals for the Fourth Circuit please go to http://www.ca4.uscourts.gov and click on Forms & Notices.(jb5, Deputy Clerk) (Entered: 02/19/2020)
02/21/2020	193	USCA Case Number 20-1191 for 191 Notice of Appeal filed by Wikimedia Foundation. Case Manager - Kirsten Hancock (jb5s, Deputy Clerk) (Entered: 02/21/2020)
03/27/2020	194	(FILED IN ERROR) NOTICE OF FILING OF OFFICIAL TRANSCRIPT of Proceedings held on 6/29/2018, before Judge T.S. Ellis, III. Court Reporter/Transcriber Tonia M. Harris, Telephone number 703-646-1438. Total number of pages filed: 30. Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date it may be obtained from the Court Reporter or through PACER. Redaction Request due 4/17/2020. Redacted Transcript Deadline set for 4/27/2020. Release of Transcript Restriction set for 6/25/2020.(bmhs, Deputy Clerk) Modified on 5/12/2020 (bmhs, Deputy Clerk). (Entered: 03/30/2020)
04/01/2020	195	(ELECTRONICALLY FILED IN ERROR)TRANSCRIPT ORDER ACKNOWLEDGMENT by Wikimedia Foundation for proceedings held on Hearing: 06/29/2018 before Judge T. NA S. Ellis, re 191 Notice of Appeal - Transcript due by 6/8/2020. (Court Reporter: Tonia Harris)(slss, Deputy Clerk) Modified on 5/11/2020 (slss, Deputy Clerk). (Entered: 04/01/2020)
05/11/2020		Set/Reset Transcript Deadlines re 195 Appeal Transcript Request. (slss, Deputy Clerk) (Entered: 05/11/2020)
05/12/2020	196	NOTICE OF FILING OF OFFICIAL TRANSCRIPT of Proceedings held on 6/29/2018, before Judge T.S. Ellis, III. Court Reporter/Transcriber Tonia M. Harris, Telephone number 703-646-1438. Total number of pages filed: 29. Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date it may be obtained from the Court Reporter or through PACER. Redaction Request due 6/2/2020. Redacted Transcript Deadline set for 6/12/2020. Release of Transcript Restriction set for 8/10/2020.(bmhs, Deputy Clerk) (Entered: 05/12/2020)
05/12/2020	197	NOTICE OF FILING OF OFFICIAL TRANSCRIPT of Proceedings held on 5/30/2019, before Judge T.S. Ellis, III. Court Reporter/Transcriber Tonia M. Harris, Telephone number 703-646-1438. Total number of pages filed: 69. Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date it may be obtained from the Court Reporter or through PACER. Redaction Request due 6/2/2020. Redacted Transcript Deadline set for 6/12/2020. Release of Transcript Restriction set for 8/10/2020.(bmhs, Deputy Clerk) (Entered: 05/12/2020)

PACER Service Center			
Transaction Receipt			
06/24/2020 09:54:38			
PACER Login:	hshamsi12:4377808:4375869	**Client Code:**	
Description:	Docket Report	**Search Criteria:**	1:15-cv-00662-TSE

Billable Pages:	30	**Cost:**	3.00

UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION
149 New Montgomery Street, 6th Floor
San Francisco, CA 94105;

NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS
1660 L Street, NW, 12th Floor
Washington, DC 20036;

HUMAN RIGHTS WATCH
350 Fifth Avenue, 34th Floor
New York, NY 10118;

AMNESTY INTERNATIONAL USA
5 Pennsylvania Plaza, 16th Floor
New York, NY 10001;

PEN AMERICAN CENTER
588 Broadway, Suite 303
New York, NY 10012;

GLOBAL FUND FOR WOMEN
222 Sutter Street, Suite 500
San Francisco, CA 94108;

THE NATION MAGAZINE
33 Irving Place, 8th Floor
New York, NY 10003;

THE RUTHERFORD INSTITUTE
P.O. Box 7482
Charlottesville, VA 22906;

WASHINGTON OFFICE ON LATIN AMERICA
1666 Connecticut Avenue, NW, Suite 400
Washington, DC 20009,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY / CENTRAL SECURITY SERVICE

FIRST AMENDED COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

Civil Action No.
15-cv-00662-TSE

Hon. T. S. Ellis, III

9800 Savage Road
Fort Meade, Anne Arundel County, MD 20755;

ADM. MICHAEL S. ROGERS, in his official capacity as Director of the National Security Agency and Chief of the Central Security Service,
National Security Agency / Central Security Service
9800 Savage Road
Fort Meade, Anne Arundel County, MD 20755;

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
Washington, DC 20511;

JAMES R. CLAPPER, in his official capacity as Director of National Intelligence,
Office of the Director of National Intelligence
Washington, DC 20511;

DEPARTMENT OF JUSTICE
950 Pennsylvania Avenue, NW
Washington, DC 20530;

LORETTA E. LYNCH, in her official capacity as Attorney General of the United States,
Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530,

Defendants.

Deborah A. Jeon
(Bar No. 06905)
jeon@aclu-md.org
David R. Rocah
(Bar No. 27315)
rocah@aclu-md.org
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND
3600 Clipper Mill Rd., #350
Baltimore, MD 21211
Phone: (410) 889-8555
Fax: (410) 366-7838

Patrick Toomey
(pro hac vice)
ptoomey@aclu.org
Jameel Jaffer
(pro hac vice)
jjaffer@aclu.org
Alex Abdo
(pro hac vice)
aabdo@aclu.org
Ashley Gorski
(pro hac vice)
agorski@aclu.org
AMERICAN CIVIL LIBERTIES UNION FOUNDATION

125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654

Charles S. Sims
(pro hac vice)
csims@proskauer.com
David A. Munkittrick
(pro hac vice)
dmunkittrick@proskauer.com
John M. Browning
(pro hac vice)
jbrowning@proskauer.com
PROSKAUER ROSE LLP
Eleven Times Square
New York, NY 10036
Phone: (212) 969-3000
Fax: (212) 969-2900

June 19, 2015

FIRST AMENDED COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

1. This lawsuit challenges the suspicionless seizure and searching of internet traffic by the National Security Agency ("NSA") on U.S. soil. The NSA conducts this surveillance, called "Upstream" surveillance, by tapping directly into the internet backbone inside the United States—the network of high-capacity cables, switches, and routers that today carry vast numbers of Americans' communications with each other and with the rest of the world. In the course of this surveillance, the NSA is seizing Americans' communications en masse while they are in transit, and it is searching the contents of substantially all international text-based communications—and many domestic communications as well—for tens of thousands of search terms. The surveillance exceeds the scope of the authority that Congress provided in the FISA Amendments Act of 2008 ("FAA") and violates the First and Fourth Amendments. Because it is predicated on programmatic surveillance orders issued by the Foreign Intelligence Surveillance Court ("FISC") in the absence of any case or controversy, the surveillance also violates Article III of the Constitution.

2. Plaintiffs are educational, legal, human rights, and media organizations that collectively engage in more than a trillion sensitive international communications over the internet each year. Plaintiffs communicate with, among many others, journalists, clients, experts, attorneys, civil society organizations, foreign government officials, and victims of human rights abuses. Plaintiff Wikimedia Foundation communicates with the hundreds of millions of individuals who visit Wikipedia webpages to read or contribute to the vast repository of human knowledge that Wikimedia maintains online. The ability to exchange information in confidence, free from warrantless government monitoring, is essential to each of

the Plaintiffs' work. The challenged surveillance violates Plaintiffs' privacy and undermines their ability to carry out activities crucial to their missions.

3. Plaintiffs respectfully request that the Court declare the government's Upstream surveillance to be unlawful; enjoin the government from continuing to conduct Upstream surveillance of Plaintiffs' communications; and require the government to purge from its databases all of Plaintiffs' communications that Upstream surveillance has already allowed the government to obtain.

JURISDICTION AND VENUE

4. This case arises under the Constitution and the laws of the United States and presents a federal question within this Court's jurisdiction under Article III of the Constitution and 28 U.S.C. § 1331. The Court also has jurisdiction under the Administrative Procedure Act, 5 U.S.C. § 702. The Court has authority to grant declaratory relief pursuant to the Declaratory Judgment Act, 28 U.S.C. §§ 2201–2202. The Court has authority to award costs and attorneys' fees under 28 U.S.C. § 2412.

5. Venue is proper in this district under 28 U.S.C. § 1391(b)(2), (e)(1).

PLAINTIFFS

6. Wikimedia Foundation ("Wikimedia") is a non-profit organization based in San Francisco, California, that operates twelve free-knowledge projects on the internet. Wikimedia's mission is to empower people around the world to collect and develop free educational content. Wikimedia does this by developing and maintaining "wiki"-based projects, and by providing the full contents of those projects to individuals around the world free of charge. Wikimedia sues on its own behalf and on behalf of its staff and users.

7. The National Association of Criminal Defense Lawyers ("NACDL") is a membership organization based in Washington, D.C. NACDL advocates for rational and humane criminal justice policies at all levels of federal, state, and local government, and seeks to foster the integrity, independence, and expertise of the criminal defense profession. NACDL sues on its own behalf and on behalf of its members.

8. Human Rights Watch ("HRW") is a non-profit, non-governmental human rights organization headquartered in New York City with offices around the world. It reports on abuses in all regions of the globe and advocates for the protection of human rights. HRW researchers conduct fact-finding investigations into human rights abuses in over 90 countries and publish their findings in hundreds of reports, multi-media products, and other documents every year, as well as through social media accounts. HRW sues on its own behalf and on behalf of its staff.

9. Amnesty International USA ("AIUSA"), headquartered in New York City, is the largest country section of Amnesty International, with hundreds of thousands of members and other supporters who work for human rights, including through national online networks, high schools, colleges, and community groups. AIUSA sues on its own behalf and on behalf of its staff and members.

10. PEN American Center ("PEN") is a human rights and literary association based in New York City. Committed to the advancement of literature and the unimpeded flow of ideas and information, PEN fights for freedom of expression; advocates on behalf of writers harassed, imprisoned, and sometimes killed for their views; and fosters international exchanges, dialogues, discussions, and debates. PEN sues on its own behalf and on behalf of its staff and members.

11. Global Fund for Women ("GFW") is a non-profit grantmaking foundation based in San Francisco, California, and New York City. GFW advances women's human rights worldwide by providing funds to women-led organizations that promote the economic security, health, safety, education, and leadership of women and girls. GFW sues on its own behalf and on behalf of its staff.

12. The Nation Magazine ("The Nation"), which is published by The Nation Company, LLC, and based in New York City, is America's oldest weekly magazine of opinion, news, and culture. It serves as a critical, independent voice in American journalism, exposing abuses of power through its investigative reporting, analysis, and commentary. In recent years, The Nation's journalists have reported on a wide range of issues relating to international affairs, including the wars in Iraq and Afghanistan, the Israel–Palestine conflict, protest activities in China and elsewhere in East Asia, and conflicts in Africa and Latin America. The Nation sues on behalf of itself, its staff, and certain of its contributing journalists.

13. The Rutherford Institute ("Rutherford") is a civil liberties organization based in Charlottesville, Virginia, committed to protecting the constitutional freedoms of Americans and the human rights of all people. Rutherford provides free legal services in defense of civil liberties and educates the public about constitutional and human rights issues. It also advocates on behalf of individuals abroad whose rights are threatened by foreign governments. Rutherford sues on its own behalf and on behalf of its staff.

14. The Washington Office on Latin America ("WOLA") is a non-profit, non-governmental organization based in Washington, D.C., that conducts research, advocacy, and education designed to advance human rights and social justice in the Americas. WOLA sues on its own behalf and on behalf of its staff.

DEFENDANTS

15. Defendant National Security Agency / Central Security Service ("NSA"), headquartered in Fort Meade, Maryland, is the agency of the United States government responsible for conducting the surveillance challenged in this case.

16. Defendant Adm. Michael S. Rogers is the Director of the NSA and the Chief of the Central Security Service. Defendant Rogers is sued in his official capacity.

17. Defendant Office of the Director of National Intelligence ("ODNI") is the agency of the United States government responsible for directing and coordinating the activities of the intelligence community, including the NSA.

18. Defendant James R. Clapper is the Director of National Intelligence ("DNI"). Together with the Attorney General, the DNI authorizes warrantless surveillance of U.S. citizens' and residents' international communications under the FAA, including Upstream surveillance. Defendant Clapper is sued in his official capacity.

19. Defendant Department of Justice ("DOJ") is one of the agencies of the United States government responsible for authorizing and overseeing surveillance conducted pursuant to the FAA, including Upstream surveillance.

20. Defendant Loretta E. Lynch is the Attorney General of the United States. Together with the DNI, the Attorney General authorizes warrantless surveillance of U.S. citizens' and residents' international communications under the FAA, including Upstream surveillance. Defendant Lynch is sued in her official capacity.

LEGAL AND FACTUAL BACKGROUND

The Foreign Intelligence Surveillance Act

21. In 1978, Congress enacted the Foreign Intelligence Surveillance Act ("FISA") to govern surveillance conducted for foreign intelligence purposes. The statute created the Foreign Intelligence Surveillance Court ("FISC") and empowered the court to grant or deny government applications for surveillance orders in certain foreign intelligence investigations.

22. Congress enacted FISA after years of in-depth congressional investigation by the committees chaired by Senator Frank Church and Representative Otis Pike, which revealed that the Executive Branch had engaged in widespread warrantless surveillance of United States citizens—including journalists, activists, and members of Congress—"who engaged in no criminal activity and who posed no genuine threat to the national security."

23. Congress has amended FISA multiple times since 1978.

24. Prior to 2007, FISA generally required the government to obtain an individualized order from the FISC before conducting electronic surveillance on U.S. soil. To obtain a traditional FISA order, the government was required to make a detailed factual showing with respect to both the target of the surveillance and the specific communications facility—often a telephone line or email account—to be monitored. The government was also required to certify that a "significant purpose" of the surveillance was to obtain foreign intelligence information. 50 U.S.C. § 1804(a)(6)(B).

25. The FISC could issue such an order only if it found, among other things, that there was probable cause to believe that "the target of the electronic surveillance is a foreign power or an agent of a foreign power," and that "each of the facilities or places at which the

electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." *Id.* § 1805(a)(2)(A)–(B).

26. The framework established by FISA remains in effect today, but it has been modified by the FAA to permit the acquisition of U.S. citizens' and residents' international communications without probable cause or individualized suspicion, as described below.

The Warrantless Wiretapping Program

27. On October 4, 2001, President George W. Bush secretly authorized the NSA to conduct a program of warrantless electronic surveillance inside the United States. This program, which was known as the President's Surveillance Program ("PSP"), was reauthorized repeatedly by President Bush between 2001 and 2007.

28. According to public statements by senior government officials, the PSP involved the warrantless interception of emails and telephone calls that originated or terminated inside the U.S. According to then-Attorney General Alberto Gonzales and then-NSA Director General Michael Hayden, NSA "shift supervisors" initiated surveillance when in their judgment there was a "reasonable basis to conclude that one party to the communication [was] a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda."

29. On January 17, 2007, then-Attorney General Alberto Gonzales publicly announced that a judge of the FISC had "issued orders authorizing the Government to target for collection international communications into or out of the United States where there [was] probable cause to believe that one of the communicants [was] a member or agent of al Qaeda or an associated terrorist organization." The Attorney General further stated that "[a]s a result of

these orders, any electronic surveillance that was occurring" as part of the PSP would thereafter "be conducted subject to the approval of the Foreign Intelligence Surveillance Court."

30. In April 2007, when the government sought reauthorization of the FISC's previous orders, a different judge of the FISC determined that key elements of the government's request were incompatible with FISA. Following the FISC's refusal to renew certain portions of its January 2007 orders, executive-branch officials appealed to Congress to amend the statute.

The Protect America Act

31. Congress enacted the Protect America Act ("PAA") in August 2007. The PAA expanded the executive's surveillance authority and provided legislative sanction for surveillance that the President had previously been conducting under the PSP. Because of a "sunset" provision, the amendments to FISA made by the PAA expired on February 17, 2008.

The FISA Amendments Act

32. President Bush signed the FISA Amendments Act ("FAA") into law on July 10, 2008. The FAA radically revised the FISA regime that had been in place since 1978 by authorizing the acquisition without individualized suspicion of a wide swath of communications, including U.S. persons' international communications, from companies inside the United States.[1]

33. In particular, the FAA allows the Attorney General and Director of National Intelligence to "authorize jointly, for a period of up to 1 year . . . the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence

[1] Plaintiffs use the term "international" to describe communications that either originate or terminate outside the United States, but not both—*i.e.*, communications that are foreign at one end.

information." 50 U.S.C. § 1881a(a). The statute requires the Attorney General, in consultation with the Director of National Intelligence, to adopt "targeting procedures" and "minimization procedures," *id.* § 1881a(d)–(e), that govern who may be targeted for surveillance by executive-branch employees and how communications are to be handled once intercepted.

34. The FISC's role in overseeing the government's surveillance under the statute consists principally of reviewing these general procedures. The FISC never reviews or approves the government's individual surveillance targets or the facilities it intends to monitor. Rather, when the government wishes to conduct surveillance under the statute, it must certify to the FISC that the court has approved its targeting and minimization procedures or that it will shortly submit such procedures for the FISC's approval. *See id.* § 1881a(g), (i). If the government so certifies, the FISC authorizes the government's surveillance for up to a year at a time. A single such order may result in the acquisition of the communications of thousands of individuals.

35. The effect of the FAA is to give the government sweeping authority to conduct warrantless surveillance of U.S. persons' international communications. While the statute prohibits the government from intentionally *targeting* U.S. persons, it authorizes the government to acquire U.S. persons' communications with the foreigners whom the NSA chooses to target. Moreover the statute does not meaningfully restrict *which* foreigners the government may target. The statute does not require the government to make any finding—let alone demonstrate probable cause to the FISC—that its surveillance targets are foreign agents, engaged in criminal activity, or connected even remotely with terrorism. The government may target any person for surveillance if it has a reasonable belief that she is a foreigner outside the United States who is likely to communicate "foreign intelligence information"—a term that is

defined so broadly as to encompass virtually any information relating to the foreign affairs of the United States. *Id.* §§ 1881a(a), 1801(e). The government may target corporations and associations under the same standard.

36. Thus, though the FAA is nominally concerned with the surveillance of individuals and groups outside the United States, it has far-reaching implications for U.S. persons' privacy. The targets of FAA surveillance may include journalists, academic researchers, human rights defenders, aid workers, business persons, and others who are not suspected of any wrongdoing. In the course of FAA surveillance, the government may acquire the communications of U.S. citizens and residents with all these persons.

THE GOVERNMENT'S IMPLEMENTATION OF THE FAA

37. The government has implemented the FAA expansively, with significant consequences for Americans' privacy. The Director of National Intelligence has reported that, in 2014, the government relied on the FAA to target 92,707 individuals, groups, or organizations for surveillance under a single court order. According to the FISC, the government gathered 250 million internet communications under the FAA in 2011 alone—at a time when the NSA had far fewer targets than it has today. Moreover, as described below, that figure does not reflect the far greater number of communications that the NSA searched for references to its targets before discarding them. Intelligence officials have declined to determine, or even estimate, how many of the communications intercepted under the FAA are to, from, or about U.S. citizens or residents. However, opinions issued by the FISC, reports by the President's Review Group on Intelligence and Communications Technologies and the Privacy and Civil Liberties Oversight Board, and media accounts indicate that FAA

surveillance results in the wide-ranging and persistent interception of U.S. persons' communications.

38. In at least one respect, the government has engaged in surveillance that exceeds even the broad authority that Congress granted in the FAA. As described below, the government has interpreted the FAA to allow it to intercept, copy, and review essentially everyone's internet communications in order to search for identifiers associated with its targets. This intrusive and far-reaching practice has no basis in the statute. The statute authorizes surveillance only of *targets'* communications; it does not authorize surveillance of everyone.

Upstream Surveillance of Internet Communications

39. The government conducts at least two kinds of surveillance under the FAA. Under a program called "PRISM," the government obtains stored and real-time communications directly from U.S. companies—such as Google, Yahoo, Facebook, and Microsoft—that provide communications services to targeted accounts.

40. This case concerns a second form of surveillance, called Upstream. Upstream surveillance involves the NSA's seizing and searching the internet communications of U.S. citizens and residents en masse as those communications travel across the internet "backbone" in the United States. The internet backbone is the network of high-capacity cables, switches, and routers that facilitates both domestic and international communication via the internet.

Background: Internet Communications

41. The internet is a global network of networks. It allows machines of different types to communicate with each other through a set of intermediating networks. At its most basic level, it consists of (1) computers and the connections between them, (2) the

communications transmitted to, by, or through those computers and connections, and (3) the rules that direct the flow of these communications.

42. All communications on the internet are broken into "packets"—discrete chunks of information that are relatively small. The packets are sent from machine to machine (and network to network) and may traverse a variety of physical circuits connecting different machines before reaching their destination. Once the packets that make up a particular communication reach their final destination, they are reassembled so that the recipient can "read" the message being sent—whether an email, a webpage, or a video.

43. Internet packets can be thought of in layers. Although computer scientists describe these layers differently depending on the context, there are three layers relevant here:

- **The Networking Layer:** The Networking Layer of a packet is like an address block on an envelope. It contains, among other things, the packet's source and destination addresses. On the internet, addresses are represented as numeric strings known as Internet Protocol ("IP") addresses. To send a packet from one IP address to another, a computer on the internet creates a packet, addresses the packet with the source and destination IP addresses, and then transmits the packet to a neighboring computer that is closer to the destination. That computer then transmits the packet to another that is closer still to the destination. This process continues until the packet reaches its destination.

- **The Transport Layer:** The Transport Layer of a packet contains information that allows it to be grouped with other packets that are part of the same session or class of communication. For example, a packet sent using the most common Transport Layer protocol (the Transmission Control Protocol ("TCP")) contains, among other things, (1) a sequence number, which allows the recipient to reassemble the packets of a communication in order, and (2) source and destination "ports," which are, in effect, internal addresses used by the sending and receiving computers.

- **The Application Layer:** The Application Layer of a packet is akin to the inside of an envelope—it contains the actual content of the communications being transmitted. If the content is too large to fit into a single packet, then the Application Layers of several different packets would need to be reassembled in order for the recipient to be able to read or interpret the communication. For example, HTTP is the Application Layer protocol used to transmit webpages. Because most websites exceed the size of a single internet packet, their contents are transmitted in a series of HTTP packets that must be reassembled before display. Other common Application Layer protocols that, like

HTTP, contain text-searchable data are SMTP (for the sending of email), IMAP and POP (for the receiving of email), and DNS (which allows computers to learn a website's IP address based on its domain name).

44. In some cases, internet packets stay on a single network (e.g., two machines in the same office talking to each other), but in other cases, the packets may traverse dozens of intermediate networks before reaching their destination. The network path can change radically and dynamically as devices and connections are added or removed from the network.

45. Often, there are multiple routes that an internet packet could follow to reach its destination. Some connected networks may be faster, cheaper, or have a wider reach. Moreover, many high-bandwidth connections route traffic based on complex contractual arrangements, which take into account factors such as cost, the type of traffic, or the balance between inbound and outbound traffic. Networks that are strategically well-connected and have high bandwidth are likely to be used for transit by packets coming from other, less-well-connected networks. These more strategically connected networks, which often link large metropolitan areas, are collectively referred to as the internet "backbone." The overwhelming majority of backbone links are fiber-optic cables, because fiber-optic connections have high bandwidth and can distribute data over long distances.

46. The internet backbone includes the approximately 49 international submarine cables that carry internet communications into and out of the United States and that land at approximately 43 different points within the country. The vast majority of international traffic into and out of the United States traverses this limited number of submarine cables.

Upstream Surveillance

47. The NSA conducts Upstream surveillance by connecting surveillance devices to multiple major internet cables, switches, and routers on the internet backbone inside the United

States. These access points are controlled by the country's largest telecommunications providers, including Verizon Communications, Inc. and AT&T, Inc. In some or all instances, aspects of Upstream surveillance may be conducted by the telecommunications providers on the government's behalf.

48. Upstream surveillance is intended to enable the comprehensive monitoring of international internet traffic. With the assistance of telecommunications providers, the NSA intercepts a wide variety of internet communications, including emails, instant messages, webpages, voice calls, and video chats. It copies and reviews substantially all international emails and other "text-based" communications—*i.e.*, those whose content includes searchable text.

49. More specifically, Upstream surveillance encompasses the following processes, some of which are implemented by telecommunications providers acting at the NSA's direction:

- **Copying.** Using surveillance devices installed at key access points along the internet backbone, the NSA makes a copy of substantially all international text-based communications—and many domestic ones—flowing across certain high-capacity cables, switches, and routers. The copied traffic includes email, internet-messaging communications, web-browsing content, and search-engine queries.

- **Filtering.** The NSA attempts to filter out and discard some wholly domestic communications from the stream of internet data, using IP filters for instance, while preserving international communications. The NSA's filtering out of domestic communications is incomplete, however, for multiple reasons. Among them, the NSA does not eliminate bundles of domestic and international communications that transit the internet backbone together. Nor does it eliminate domestic communications that happen to be routed abroad.

- **Content Review.** The NSA reviews the copied communications—including their full content—for instances of its search terms. The search terms, called "selectors," include email addresses, phone numbers, IP addresses, and other identifiers that NSA analysts believe to be associated with foreign intelligence targets. Again, the NSA's targets are not limited to suspected foreign agents and terrorists, nor are its selectors limited to individual email addresses. The NSA may monitor or "task" selectors used by large

groups of people who are not suspected of any wrongdoing—such as the IP addresses of computer servers used by hundreds of different people.

- **Retention and Use.** The NSA retains all communications that contain selectors associated with its targets, as well as those that happened to be bundled with them in transit. As discussed further below, NSA analysts may read, query, data-mine, and analyze these communications with few restrictions, and they may share the results of those efforts with the FBI, including in aid of criminal investigations.

50. One aspect of the processes outlined above bears emphasis: Upstream surveillance is not limited to communications sent or received by the NSA's targets. Rather, it involves the surveillance of essentially *everyone's* communications. The NSA systematically examines the full content of substantially all international text-based communications (and many domestic ones) for references to its search terms. In other words, the NSA copies and reviews the communications of millions of innocent people to determine whether they are discussing or reading anything containing the NSA's search terms. The NSA's practice of reviewing the *content* of communications for selectors is sometimes called "about" surveillance. This is because its purpose is to identify not just communications that are to or from the NSA's targets but also those that are merely "about" its targets. This is the digital analogue of having a government agent open every piece of mail that comes through the post to determine whether it mentions a particular word or phrase. Most pieces of mail—or email—will contain nothing of interest, but the government must still look through each one to find out. Although it could do so, the government makes no meaningful effort to avoid the interception of communications that are merely "about" its targets; nor does it later purge those communications.

51. Prior to the summer of 2013, the government had not publicly disclosed the fact that, under the FAA, it routinely reviews communications that are neither to nor from its targets. As the Privacy and Civil Liberties Oversight Board observed, "The fact that the

government engages in such collection is not readily apparent from the face of the statute, nor was collection of information 'about' a target addressed in the public debate preceding the enactment of FISA or the subsequent enactment of the FISA Amendments Act."

Targeting and Minimization Procedures

52. As indicated above, the FAA requires the government to adopt targeting and minimization procedures that govern who may be targeted for surveillance by executive-branch employees and how communications are to be handled once intercepted. These procedures are extremely permissive, and to the extent they impose limitations, those restrictions are riddled with exceptions.

53. Nothing in the targeting procedures meaningfully constrains the government's selection of foreign targets. Nor do the targeting procedures require the government to take measures to avoid intercepting U.S. persons' international communications. The targeting procedures expressly contemplate "about" surveillance, and thus the interception and review of communications between non-targets.

54. The minimization procedures are equally feeble. They impose no affirmative obligation on the NSA to promptly identify and purge U.S. persons' communications once they have been obtained. Rather, they allow the NSA to retain communications gathered via Upstream surveillance for as long as three years by default. It can retain those communications indefinitely if the communications are encrypted; if they are found to contain foreign intelligence information (again, defined broadly); or if they appear to be evidence of a crime. Indeed, the NSA may even retain and share wholly domestic communications obtained through the accidental targeting of U.S. persons if the NSA determines that the communications contain "significant foreign intelligence information" or evidence of a crime. The minimization

procedures also expressly contemplate that the NSA will intercept, retain, and disseminate attorney-client privileged communications. The minimization procedures bar the NSA from querying Upstream data using identifiers associated with specific U.S. persons, but they do not otherwise prohibit the NSA from conducting queries designed to reveal information to, from, or about U.S. persons.

The Surveillance of Plaintiffs

55. Plaintiffs are educational, legal, human rights, and media organizations. Their work requires them to engage in sensitive and sometimes privileged communications, both international and domestic, with journalists, clients, experts, attorneys, civil society organizations, foreign government officials, and victims of human rights abuses, among others.

56. By intercepting, copying, and reviewing substantially all international text-based communications—and many domestic communications as well—as they transit telecommunications networks inside the United States, the government is seizing and searching Plaintiffs' communications in violation of the FAA and the Constitution.

57. The conclusion that the government is seizing and searching Plaintiffs' communications is well-founded for at least four reasons.

58. First, the sheer volume of Plaintiffs' communications makes it virtually certain that the NSA has intercepted, copied, and reviewed at least some of their communications. In the course of a year, Plaintiffs collectively engage in more than one trillion international internet communications. As explained further below, Upstream surveillance could achieve the government's stated goals only if it entailed the copying and review of a large percentage of international text-based traffic. However, even if one assumes a 0.00000001% chance—one one-hundred millionth of one percent—of the NSA copying and reviewing any particular

communication, the odds of the government copying and reviewing at least one of the Plaintiffs' communications in a one-year period would be greater than 99.9999999999%.

59. In reality, this calculation understates the likelihood that the NSA has intercepted, copied, and reviewed Plaintiffs' communications, because large swaths of internet traffic that are not amenable to the text-based searches conducted in the course of Upstream surveillance and are likely of no foreign-intelligence interest to the government. By some estimates, for example, two-thirds of internet traffic consists of video traffic. The NSA could readily configure its surveillance equipment to ignore that traffic, or at least the significant portions of it (e.g., Netflix traffic) that are almost certainly of no interest. Because of the substantial efficiency gains to be had, it is extremely likely that the government engages in this kind of filtering, allowing it to more comprehensively monitor text-searchable traffic like that of Plaintiffs.

60. Second, the geographic distribution of Plaintiffs' contacts and communications across the globe makes it virtually certain that the NSA has intercepted, copied, and reviewed Plaintiffs' communications. As noted above, the internet backbone includes the approximately 49 international submarine cables carrying the vast majority of internet traffic into and out of the United States. It also includes the limited number of high-capacity terrestrial cables that carry traffic between major metropolitan areas within the United States, or between the United States and Canada or Mexico. The junctions where these backbone cables meet are in essence "chokepoints"—because almost all international internet traffic (as well as a significant share of domestic traffic) flows through one or more of them. Prime examples are the points where international submarine cables come ashore. The government has acknowledged using

Upstream surveillance to monitor communications at "international Internet link[s]" on the internet backbone.

61. Given the relatively small number of international chokepoints, the immense volume of Plaintiffs' communications, and the fact that Plaintiffs communicate with individuals in virtually every country on earth, Plaintiffs' communications almost certainly traverse every international backbone link connecting the United States with the rest of the world.

62. Third, and relatedly, in order for the NSA to reliably obtain communications to, from, or about its targets in the way it has described, the government must be copying and reviewing all the international text-based communications that travel across a given link. That is because, as a technical matter, the government cannot know beforehand which communications will contain selectors associated with its targets, and therefore it must copy and review all international text-based communications transiting that circuit in order to identify those of interest. As the Privacy and Civil Liberties Oversight Board explained with respect to Upstream surveillance, "Digital communications like email, however, enable one, as a technological matter, to examine the contents of all transmissions passing through collection devices and acquire those, for instance, that contain a tasked selector anywhere within them." Because backbone cables carry vast amounts of internet traffic, the number of communications whose contents will be copied and reviewed will be enormous, regardless of how many the government ultimately retains.

63. There is an even more basic reason that, in conducting Upstream surveillance, the government must be monitoring all the international text-based communications that travel across a given link. To search the contents of any text-based communication for instances of the NSA's "selectors" as that communication traverses a particular backbone link, the

government must first copy and reassemble all of the packets that make up that communication. Those packets travel independently of one another, intermingled with packets of other communications in the stream of data. Where the government seeks to identify communications to, from, or about its many targets, as it does using Upstream surveillance, the packets of interest cannot be segregated from other, unrelated packets in advance. Rather, in order to reliably intercept the communications it seeks, the government must first copy *all* such packets traversing a given backbone link, so that it can reassemble and review the transiting communications in the way it has described.

64. In short, for every backbone link that the NSA monitors using Upstream surveillance, the monitoring must be comprehensive in order for the government to accomplish its stated goals. Accordingly, even if the NSA conducts Upstream surveillance on only a single internet backbone link, it must be intercepting, copying, and reviewing at least those communications of Plaintiffs traversing that link. In fact, however, the NSA has confirmed that it conducts Upstream surveillance at more than one point along the internet backbone, through the compelled assistance of multiple major telecommunications companies.

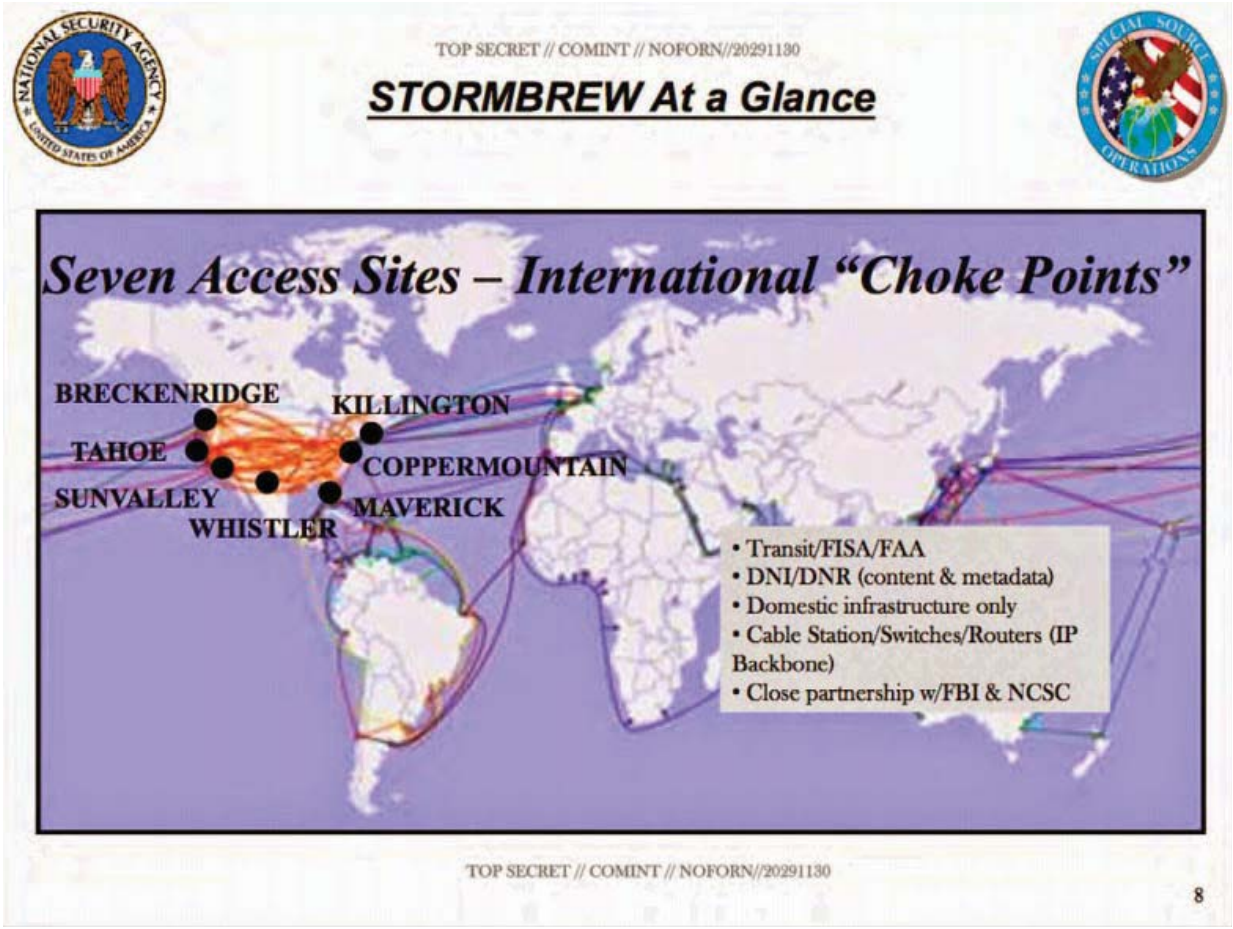
65. Fourth, given the way the government has described Upstream surveillance, it has a strong incentive to intercept communications at as many backbone chokepoints as possible. The government's descriptions of Upstream surveillance make clear that the government is interested in obtaining, with a high degree of confidence, all international communications to, from, or about its targets. For example, the Privacy and Civil Liberties Oversight Board has described the use of Upstream surveillance to collect "about" communications as "an inevitable byproduct of the government's efforts to comprehensively acquire communications that are sent to or from its targets." And it has said about Upstream

surveillance more generally that its "success . . . depends on collection devices that can reliably acquire data packets associated with the proper communications."

66. If the government's aim is to "comprehensively" and "reliably" obtain communications to, from, and about targets scattered around the world, it must conduct Upstream surveillance at many different backbone chokepoints. That is especially true because the communications of individual targets may take multiple paths when entering or leaving the United States. When two people communicate in real-time, the communications they exchange frequently take different routes across the internet backbone, even though the end-points are the same. In other words, in the course of a single exchange, the communications *from* a target frequently follow a different path than those *to* the target. Relatedly, a target's location may vary over time, as do the network conditions that determine a given communication's path from origin to destination. As a result, a target's communications may traverse one backbone cable or chokepoint at one moment, but a different one later. In fact, as the Privacy and Civil Liberties Oversight Board observed, even a single email "can be broken up into a number of data packets that take different routes to their common destination." Because of these variables, Upstream surveillance would be comprehensive only if it were implemented at a number of backbone chokepoints.

67. For the four reasons stated above, it is a virtual certainty that the NSA is intercepting, copying, and reviewing Plaintiffs' communications.

68. This conclusion is corroborated by government documents that have been published in the press. For example, one NSA slide illustrates the Upstream surveillance facilitated by just a single provider (referred to as "STORMBREW") at seven major international chokepoints in the United States:



69. Similarly, another NSA document states that, in support of FAA surveillance, the "NSA has expended a significant amount of resources to create collection/processing capabilities at many of the chokepoints operated by U.S. providers through which international communications enter and leave the United States." In fact, in describing the scale and operation of Upstream surveillance, *The New York Times* has reported, based on interviews with senior intelligence officials, that "the N.S.A. is temporarily copying and then sifting through the contents of what is apparently most e-mails and other text-based communications that cross the border."

70. The government's interception, copying, and review of Plaintiffs' communications while in transit is a violation of Plaintiffs' reasonable expectation of privacy in

those communications. It is also a violation of Plaintiffs' right to control those communications and the information they reveal and contain.

71. Furthermore, because of the nature of their communications, and the location and identities of the individuals and groups with whom and about whom they communicate, there is a substantial likelihood that Plaintiffs' communications intercepted by the NSA through Upstream surveillance are retained, read, and disseminated.

72. The retention, reading, and dissemination of Plaintiffs' communications is a further, discrete violation of Plaintiffs' reasonable expectation of privacy in those communications. It is also a further, discrete violation of Plaintiffs' right to control those communications and the information they reveal and contain.

73. Plaintiffs, in connection with constitutionally protected activities, communicate with people whom the government is likely to target when conducting Upstream surveillance, including foreign government officials, journalists, experts, human rights defenders, victims of human rights abuses, and individuals believed to have information relevant to counterterrorism efforts.

74. A significant amount of the information that Plaintiffs exchange over the internet is "foreign intelligence information" within the meaning of the FAA.

75. Because of ongoing government surveillance, including Upstream surveillance, Plaintiffs have had to take burdensome and sometimes costly measures to minimize the chance that the confidentiality of their sensitive information will be compromised. Plaintiffs have variously had to develop new protocols for transmitting sensitive information, to travel long distances to collect information that could otherwise have been shared electronically, and in some circumstances to forgo particularly sensitive communications altogether.

76. Because of ongoing government surveillance, including Upstream surveillance, Plaintiffs are not able to gather and relay information, represent their clients, and engage in domestic and international advocacy as they would in the absence of the surveillance. Upstream surveillance reduces the likelihood that clients, users, journalists, witnesses, experts, civil society organizations, foreign government officials, victims of human rights abuses, and other individuals will share sensitive information with Plaintiffs.

77. Upstream surveillance is inhibiting the constitutionally protected communications and activities of Plaintiffs and others not before the Court.

Wikimedia Foundation

78. Wikimedia is a non-profit organization dedicated to encouraging the growth, development, and distribution of free, multilingual, educational content. In this effort, it develops and maintains "wiki"-based projects, and provides the full contents of those projects to individuals around the world free of charge. At present, Wikimedia operates twelve free-knowledge projects ("Projects") as well as other related websites and pages on the internet.

79. The best-known of Wikimedia's Projects is Wikipedia—a free internet encyclopedia that is one of the top ten most-visited websites in the world and one of the largest collections of shared knowledge in human history. In 2014, Wikipedia contained more than 33 million articles in over 275 languages, and Wikimedia sites received between approximately 412 and 495 million monthly visitors. Wikipedia's content is collaboratively researched and written by millions of volunteers, many of whom choose not to identify themselves, and is in most instances open to editing by anyone. Volunteers also use Wikipedia discussion forums and "discussion pages" to debate the editorial policies and decisions required for reliable and neutral content.

80. Other Projects include Wikimedia Commons, an online repository of free images, sound, and other media files; Wikinews, a collaborative journalism platform for volunteers to create and edit original news articles; and Wikibooks, a platform for the creation of free textbooks and annotated texts that anyone can edit consistent with the policies of the site.

81. Wikimedia encourages individuals around the world to contribute to the Projects by communicating information to Wikimedia. Wikimedia receives and maintains this information, and subsequently communicates it to the many other individuals who seek to access, engage with, and further add to Wikimedia's store of knowledge. The principal way in which Wikimedia communicates with its community—which, at its broadest level, consists of individuals who access or contribute to the body of knowledge comprising the twelve Projects—is via the internet.

82. Wikimedia provides the technical infrastructure for the Projects, much of which is hosted on Wikimedia's servers in Virginia, Texas, and California. In addition, Wikimedia develops software and provides tools for others to develop software platforms; develops mobile phone applications and enters into partnerships; administers grants to support activity that benefits the Wikimedia user community and the Wikimedia movement; provides administrative support to grantees; works with community members to organize conferences and community-outreach events globally; and engages in advocacy on issues that affect the Wikimedia community.

83. Wikimedia maintains an active and close relationship with the volunteers, contributors, and many other users who comprise the Wikimedia community. Wikimedia exists for this community and depends upon it: the user community plays a vital role in many of

Wikimedia's functions, including the creation of Wikimedia content, the development and enforcement of Wikimedia policies, the donation of funds that help Wikimedia thrive, and the governance of the organization as a whole. In short, Wikimedia operates interdependently with its user community in pursuit of a shared set of free-knowledge values.

84. Wikimedia's corporate structure and decision-making reflect this interdependence. In accordance with Wikimedia's bylaws, at least half of Wikimedia's Board of Trustees is selected by Wikimedia community members. That Board relies, in turn, on several user-staffed committees to oversee Board elections, consider grant applications, and recommend new Wikimedia chapters or community organizations. More generally, Wikimedia makes core organizational decisions after soliciting the input and preferences of its users on topics including its public-policy positions, the creation of new features and Projects, corporate strategy, and budgetary matters. For instance, Wikimedia staff frequently engage in "Community Consultations," in which community members can offer their views on these and other matters directly.

85. Wikimedia's community of volunteers, contributors, and readers consists of individuals in virtually every country on earth. Among many others, the Wikimedia community includes U.S. persons who are located abroad and who engage in international communications with Wikimedia.

86. Upstream surveillance implicates at least three categories of Wikimedia communications: (i) Wikimedia communications with its community members, who read and contribute to Wikimedia's Projects and webpages, and who use the Projects and webpages to interact with each other; (ii) Wikimedia's internal "log" communications, which help it to

monitor, study, and improve its community members' use of the Projects; and (iii) communications by Wikimedia staff.

87. As the operator of one of the most-visited websites in the world, Wikimedia engages in an extraordinarily high volume of internet communications. From April 1, 2014 to March 31, 2015, Wikimedia websites received over 255 billion "page views." Over the lifespan of the Wikimedia Projects, Wikimedia's users have edited its pages more than two billion times. Each of these activities involves internet communications between Wikimedia and its users—the majority of whom are located abroad.

88. Indeed, Wikimedia engages in more than one trillion international communications each year, with individuals who are located in virtually every country on earth. For a user to view, search, log in, edit, or contribute to a Wikimedia Project webpage, the user's device must send at least one HTTP or HTTPS "request" to a Wikimedia server. "HTTP" and "HTTPS" are common protocols for transmitting data via the internet, including the content of many webpages. The number of requests required for a user to access a particular webpage depends on the number of graphics, videos, and other specialized components featured on the page. After receiving such a user request, the Wikimedia server transmits an HTTP or HTTPS "response" to the user's device, where the content of the requested webpage component is rendered and displayed to the user. In May 2015, Wikimedia's U.S.-based servers received more than 88 billion HTTP or HTTPS requests from outside the United States. At this rate, Wikimedia receives more than one trillion HTTP or HTTPS requests annually, and transmits more than one trillion HTTP or HTTPS responses back to those Wikimedia users abroad.

89. Wikimedia's HTTP and HTTPS communications are essential to its organizational mission, as is its ability to control and maintain the privacy of these communications. The communications reveal and contain some of the most sensitive information that Wikimedia possesses: which specific webpages each particular person is editing or visiting. In other words, they reveal who is reading—or writing—what.

90. For example, among other private information, HTTP and HTTPS requests reveal or contain the user's IP address; the URL of the webpage sought by the user, which often conveys information about the content of the requested page; and the "user agent," which may identify the manufacturer, model, version, and other information about the user's device. Many requests also contain other types of private information, such as a user's log-in credentials; the referrer, which reflects information about the previous webpage the user visited; the search terms a user entered to query Wikimedia's webpages; "cookies," which include information that can be used to link a user to his or her prior Wikimedia requests and prior approximate geolocation; a user's non-public "draft" contributions to Wikimedia; or a user's private questions, comments, or complaints, submitted via Wikimedia's online feedback platform.

91. In much the same way, Wikimedia's HTTP and HTTPS responses may reveal or contain, among other private information, the user's IP address; the content of the requested webpage component; the URL of the webpage the user should be redirected to; "cookies," which include information used to link a user to subsequent Wikimedia requests and his or her approximate geolocation; search terms; a user's username; a user's non-public "draft" contributions; and a user's private questions, comments, or complaints.

92. In furtherance of its mission, Wikimedia also frequently engages in communications that permit its users to interact with one another more directly. For example, a

registered user of Wikimedia may send an email via Wikimedia to another registered user, so long as both have enabled email communications on their Wikimedia accounts. Similarly, Wikimedia engages in communications that allow users to interact in small or limited groups—including over wikis that only certain users, such as user-community leaders, have access to, and mailing lists with restricted membership. Some of these communications are transmitted via HTTP or HTTPS; others rely on different protocols. All of these interactions involve communications between Wikimedia and its community members.

93. The second category of Wikimedia communications are its internal, proprietary "log" communications, which help it to monitor, study, and improve the Projects. In particular, every time Wikimedia receives an HTTP or HTTPS request from a person accessing a Project webpage, it creates a corresponding log entry. Among other private information, logs contain the user's IP address; the URL of the webpage sought by the user; the time the request was received by Wikimedia's server; and the "user agent," which may identify the manufacturer, model, version, and other information about the user's device. Depending on the location of the user and the routing of her request, the log may be generated by Wikimedia's servers abroad, which in turn send the log to Wikimedia in the United States. In May 2015, Wikimedia transmitted more than 140 billion logs from its servers abroad to its servers in the United States. The organization relies on its logs for a variety of analytical projects, which are designed to improve Wikimedia's operations and the experience of those using the Projects.

94. Wikimedia's communications with its community members—as well as its internal logs—link each user's page views, searches, and contributions with his or her IP address, as well as with other user-specific information. As a rule, Wikimedia maintains as private the IP addresses associated with its community members and their individual

interactions with the Projects, except in those instances where an individual editor reveals his or her IP address publicly (i.e., is not logged in as a registered user). IP addresses, like telephone numbers, are often personally identifying, especially in conjunction with other information about a given communication or internet user. It is generally trivial to link a particular IP address with a particular person—thereby revealing his or her online activities—in part because internet service providers routinely maintain records of the IP addresses assigned to their network subscribers over time.

95. Because of the information they contain, Wikimedia's communications with its community members, as well as its internal communications related to the study and improvement of the Projects, are often sensitive and private. These communications reveal a detailed picture of the everyday concerns and reading habits of Wikimedia's users, and often constitute a record of their political, religious, sexual, medical, and expressive interests.

96. Seizing and searching Wikimedia's communications is akin to seizing and searching the patron records of the largest library in the world—except that Wikimedia's communications provide a more comprehensive and detailed picture of its users' interests than any previous set of library records ever could have offered.

97. Upstream surveillance permits the government to observe—continuously—which of Wikimedia's millions of webpages are being read or edited at any given moment, and by whom. Moreover, it allows the government to review those communications for any reference to its tens of thousands of search terms, and to retain a copy of any communication that is of interest.

98. As an organization, Wikimedia has an acute privacy interest in its communications—one on par with that of users themselves. That is because Wikimedia's

mission and existence depend on its ability to ensure that readers and editors can explore and contribute to the Projects privately when they choose to do so. Wikimedia's communications reveal who has contributed to the Projects or visited them in search of information—and, just as importantly, exactly *what* information Wikimedia has exchanged with any individual user. With the partial exception of editors who publicly disclose their IP addresses, these exchanges are not public; they are private interactions between Wikimedia and its community members. If it were otherwise, Wikimedia would have immense difficulty both gathering content and sharing information as widely as possible. This privacy is necessary to foster trust with community members and to encourage the growth, development, and distribution of free educational content.

99. Wikimedia's communications also reveal private information about its operations, including details about its technical infrastructure, its data flows, and its member community writ large.

100. Wikimedia takes steps to protect the privacy of its communications and the confidentiality of the information it thereby receives. For instance, because of the sensitivity of Wikimedia's communications with its community members, Wikimedia seeks to collect and retain as little information about those exchanges as possible. Where it does collect such information, Wikimedia strives to keep it for only a limited amount of time, consistent with the maintenance, understanding, and improvement of the Projects and with Wikimedia's legal obligations. Still, Wikimedia possesses a large volume of sensitive information about its interactions with its community members, and it transmits a large volume of sensitive information about those interactions every day.

101. Wikimedia defends the privacy of its communications in other ways, including through both technical measures and legal action. Wikimedia undertakes costly and burdensome measures to ensure the security of its communications and the data it retains as a result. Wikimedia also assures its community via policies, public statements, and guidelines that it will reject third-party requests for non-public user information unless it is legally required to disclose that information. In keeping with these assurances, Wikimedia resists third-party demands for information that are overly broad, unclear, or irrelevant; notifies users individually of information requests when legally permitted; and provides legal defense funds for certain community members who are subject to lawsuits or demands for non-public information as a result of their participation in the Projects.

102. Wikimedia also engages in a third category of sensitive communications. Certain members of Wikimedia's staff routinely engage in sensitive, confidential, and privileged internet communications with non-U.S. persons located abroad in carrying out Wikimedia's work.

103. Wikimedia's communications—with its community members, its internal communications, and its staff communications—are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of Wikimedia, its staff, and its users, and it violates their right to control those communications and the information they contain.

104. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates Wikimedia's international communications because Wikimedia is communicating with or about persons the government has targeted for Upstream surveillance. Wikimedia's international contacts include foreign telecommunications companies, foreign government

officials, political and business leaders, universities, Wikimedia users and their legal counsel, Wikimedia trustees and international contractors, Wikimedia's international outside legal counsel, project partners, grantees, and volunteers—some of whom are likely targets. Wikimedia's communications with these contacts sometimes concern topics that fall within the FAA's expansive definition of "foreign intelligence information." Wikimedia communicates both with and about these likely targets. Wikimedia's international communications contain, among other things, information about its foreign contacts, including the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to Wikimedia's work.

105. Moreover, more than one trillion of Wikimedia's international communications each year—its HTTP and HTTPS transmissions as well as its internal logs of user activity—contain details such as website addresses and IP addresses. Whenever a Wikimedia user abroad edits or contributes to a Project webpage that happens to reference one of the NSA's selectors, Wikimedia engages in an international communication containing that selector. The same is often true when a Wikimedia user abroad simply reads such a Project webpage. Some of these communications are likely retained, read, and disseminated in the course of Upstream surveillance.

106. Because Wikipedia is a comprehensive encyclopedic resource, it includes entries related to virtually any foreign organization or company the U.S. government might target for Upstream surveillance. Many of these entries contain website addresses and domain names associated with those likely targets. Notably, website addresses or domain names associated with organizations on the U.S. State Department's Foreign Terrorist Organization list appear over 700 times on Project webpages—including those describing organizations, like

Uzbekistan's Islamic Jihad Union, whose communications the U.S. government has targeted using FAA surveillance.

107. The NSA has expressed interest in surveilling Wikimedia's communications. An NSA slide disclosed by the media asks, "Why are we interested in HTTP?" It then answers its own question: "Because nearly everything a typical user does on the Internet uses HTTP." This statement is surrounded by the logos of major internet companies and websites, including Facebook, Yahoo, Twitter, CNN.com, and Wikipedia. The slide indicates that, by monitoring HTTP communications, the NSA can observe "nearly everything a typical user does" online—including individuals' online reading habits and other internet activities. This information is queried and reviewed by analysts using a search tool that allows NSA analysts to examine data intercepted pursuant to the FAA and other authorities.

108. Upstream surveillance undermines Wikimedia's ability to conduct its work. Wikimedia depends on its ability to ensure anonymity for individuals abroad who view, edit, or otherwise use Wikimedia Projects and related webpages. The ability to read, research, and write anonymously is essential to the freedoms of expression and inquiry. In addition, Wikimedia's staff depend on the confidentiality of their communications, including in some cases their ability to ensure that their contacts' identities will not be revealed. Because of these twin needs for anonymity and confidentiality, Upstream surveillance harms the ability of Wikimedia's staff to engage in communications essential to their work and compromises Wikimedia's organizational mission by making online access to knowledge a vehicle for U.S. government monitoring.

109. Due in part to NSA surveillance, including Upstream surveillance, Wikimedia has undertaken burdensome and costly measures to protect its communications, including adopting more secure methods of electronic communication, and in some instances self-censoring communications or forgoing electronic communications altogether. These measures divert Wikimedia's time and monetary resources as a non-profit entity from other important organizational work.

110. Despite these precautions, Wikimedia believes that Upstream surveillance has resulted and will result in some foreign readers, editors, contributors, and volunteers being less willing to read, contribute to, or otherwise engage with Wikimedia's Projects. For instance, some Wikimedia users have expressed reluctance to continue participating in the Wikimedia movement because of U.S. government surveillance, including FAA surveillance. The loss of these foreign users is a direct detriment to Wikimedia, its ability to receive information and associate with its community members, and its organizational goal of increasing global access

to knowledge. It also harms Wikimedia's domestic users, who do not have access to information and opinions that Wikipedia's foreign contributors would otherwise have provided. Similarly, Wikimedia believes that Upstream surveillance reduces the likelihood that Wikimedia's foreign volunteers, grantees, and other contacts will communicate with staff members, because they fear that their communications will be intercepted by the U.S. government and also shared with the other governments, intelligence services, and organizations with which the U.S. government cooperates.

111. Because Wikimedia's community members are so numerous, because they are dispersed across the globe, and because millions of them choose to interact with Wikimedia anonymously, their rights are likely to be impaired if Wikimedia is unable to assert claims on their behalf. That is especially so because Wikimedia is uniquely capable of presenting the aggregate effects that Upstream surveillance has on community members' ability to contribute to the Projects and to receive information from others.

National Association of Criminal Defense Lawyers

112. The National Association of Criminal Defense Lawyers ("NACDL") is a membership organization based in Washington, D.C. NACDL's mission is to foster the integrity, independence, and expertise of the criminal defense profession, and to promote the proper and fair administration of justice. NACDL has approximately 9,200 members as well as 90 local, state, and international affiliate organizations with approximately 40,000 members. NACDL's interest in challenging the lawfulness of Upstream surveillance is germane to the organization's mission and purpose, and to its relationship with its members. As explained below, because unlawful U.S. government surveillance profoundly affects the ability of

criminal defense attorneys to ensure that accused persons receive effective counsel, such surveillance interferes with the proper and fair administration of justice.

113. As defense attorneys, NACDL's members engage in international and domestic internet communications that are essential to the effective representation of their clients. Among other things, NACDL's members routinely engage in sensitive, confidential, and privileged internet communications with non-U.S. persons located abroad as part of their representations.

114. The communications of NACDL's members are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of members' communications and it violates their right to control their communications and the information they contain.

115. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates international communications of NACDL's members because they are communicating with or about persons the government has targeted for Upstream surveillance. In the course of their representations, NACDL members communicate internationally with clients, clients' families, witnesses, journalists, human rights organizations, experts, investigators, and foreign government officials, some of whom are likely targets. Their communications with these contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." NACDL members communicate both with and about these likely targets. Members' international communications contain, among other things, details about their foreign contacts and other important sources of information—details such as the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to their work.

116. One group of NACDL members is especially likely to have their communications retained, read, and disseminated in the course of Upstream surveillance: defense attorneys who represent individuals in criminal prosecutions in which the government has acknowledged its use FAA surveillance. In these cases, the government's prosecution of the defendant is based on evidence obtained from an FAA target. As a result, defense attorneys are especially likely to engage in communications to, from, or about FAA targets in the course of investigating the government's allegations, contacting witnesses, and collecting their own evidence. Indeed, in several of these cases, the targeted selector—*e.g.*, the targeted email address—has been identified in press reports or may be ascertained from congressional testimony and court filings. NACDL defense attorneys who communicate internationally with or about that targeted selector will have their communications retained by the government, much as their clients' communications were warrantlessly intercepted and retained.

117. NACDL members have an ethical obligation to protect the confidentiality of their clients' information, including information covered by the attorney-client privilege.

118. Upstream surveillance compromises NACDL members' ability to comply with their ethical obligations and undermines their effective representation of their clients. Members' defense work depends on the confidentiality of their communications, including their ability to assure contacts that their communications—and, in some cases, even their identities—will not be revealed. Due in part to NSA surveillance, including Upstream surveillance, NACDL's members have undertaken burdensome and costly measures to protect their communications, including adopting more secure methods of electronic communication, traveling to conduct in-person meetings, and in some instances avoiding sensitive topics or forgoing communications altogether. Despite these precautions, NACDL believes that

Upstream surveillance reduces the likelihood that potential sources, witnesses, experts, and foreign government officials will share sensitive information with NACDL's members, because those contacts fear that their communications will be intercepted by the U.S. government and also shared with the other governments, intelligence services, and organizations with which the U.S. government cooperates.

NACDL Member Joshua L. Dratel

119. Joshua L. Dratel is a nationally recognized criminal defense lawyer in New York City who has been a member of NACDL since 1985. He is Chair of NACDL's National Security Committee, co-Chair of NACDL's Select Committee on Military Tribunals, and Co-Chair of its Amicus Curiae Committee. From 2003 to 2009, he served as a member of the Board of Directors of NACDL. He is also co-editor of *The Torture Papers: The Legal Road to Abu Ghraib* (Cambridge University Press 2005).

120. Mr. Dratel's litigation experience encompasses all aspects of criminal defense, and among other clients, he represents individuals accused of internet- and terrorism-related crimes. For example, he defended Wadith El Hage in *United States v. Usama Bin Laden*, the prosecution resulting from the 1998 bombings of the U.S. embassies in Kenya and Tanzania. Mr. Dratel also represented David Hicks—who was detained at Guantánamo Bay for six years—in U.S. military commission proceedings. The U.S. Court of Military Commission Review recently overturned Mr. Hicks's conviction for material support for terrorism. Mr. Dratel's current clients include Baasaly Moalin, who is appealing from a conviction of charges of material support for terrorism.

121. Mr. Dratel's law practice also includes a client who has received notice of FAA surveillance, and he previously represented a client in another case where officials have told

Congress that the government used FAA surveillance in the course of its investigation. He has defended other individuals in prosecutions where there is reason to believe the government relied on such surveillance.

122. In connection with his defense work and confidential consultations with defense attorneys in other national security-related cases, Mr. Dratel routinely engages in both domestic and international communications via the internet. Many of the individuals with whom he exchanges information are located abroad, and are neither U.S. citizens nor permanent residents. Their communications occur via email, instant messenger, and text messaging.

123. The vast majority of Mr. Dratel's international communications as a defense attorney are sensitive, and many of them are privileged or otherwise protected from disclosure by the attorney work-product doctrine.

124. Mr. Dratel's communications are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of his communications and it violates his right to control his communications and the information they contain.

125. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates Mr. Dratel's international communications because he is communicating with persons the government has targeted for Upstream surveillance. In the course of his representations, Mr. Dratel communicates internationally with clients, clients' families, lawyers, witnesses, journalists, human rights organizations, experts, investigators, and foreign government officials, some of whom are likely targets. Most notably, his international contacts include individuals the U.S. government has targeted for prosecution for terrorism-related crimes, as well as their families, friends, and associates, including their attorneys overseas. For example, Mr. Dratel communicates via the internet with his former client, Mr. Hicks, who lives

in Australia following his release from Guantánamo Bay. In addition, Mr. Dratel's communications with his international contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." Mr. Dratel also communicates with likely FAA targets when he visits websites hosted overseas on the internet. This internet browsing involves communications with selectors—such as domain names and IP addresses—that the NSA has likely targeted for FAA surveillance. In his representation of defendants charged with terrorism-related crimes, it is often necessary for him to review websites maintained by terrorist organizations abroad, so that he can understand the facts related to certain investigations and prosecutions.

126. Similarly, there is a substantial likelihood that the NSA retains, reads, and disseminates Mr. Dratel's international communications because he is communicating *about* persons the government has targeted for Upstream surveillance. Mr. Dratel's international communications contain, among other things, details about his foreign contacts and other important sources of information—details such as the email addresses, phone numbers, social media identities, and website addresses of foreign individuals and organizations relevant to his work.

127. The fact that Mr. Dratel's clients have been subject to FAA surveillance themselves, or involved in investigations where others were subject to such surveillance, makes the NSA's retention and dissemination of Mr. Dratel's own communications especially likely. In representing these clients, Mr. Dratel is almost certain to engage in communications to, from, or about FAA targets in the course of investigating the government's allegations, contacting witnesses, and collecting evidence abroad via the internet. When Mr. Dratel

communicates with or about persons and selectors targeted under the FAA, he is subject to FAA surveillance just like his clients.

128. Due in part to U.S. government surveillance, including Upstream surveillance, Mr. Dratel has had to undertake burdensome and costly measures to protect his international communications, and in certain instances has forgone those communications altogether. For example, Mr. Dratel has had to and will have to travel abroad to gather information in-person that he would otherwise have gathered by electronic communication. Such travel is time-consuming and costly. He has also paid for and will have to pay for investigators abroad to travel to the United States to meet with him in-person to discuss their cases. In addition, Mr. Dratel routinely relies on time-consuming security measures, such as Pidgin Encryption and PGP, to encrypt his domestic and international instant messages and emails, in an effort to protect especially sensitive privileged communications and work product. Mr. Dratel also routinely censors his own speech (and asks his international contacts to do the same) in electronic communications. These precautions and security measures are not voluntary; they are the result of Upstream surveillance and the rules of professional responsibility that apply to Mr. Dratel as an attorney.

129. As a general matter, Upstream surveillance compromises Mr. Dratel's ability to communicate with his clients overseas and to gather information relevant and necessary to his work. This surveillance makes it difficult, expensive, and sometimes impossible to obtain information from individuals outside of the United States. In some instances, the increased awareness of U.S. government surveillance has resulted and will result in clients, lawyers, and potential witnesses limiting the information that they share with Mr. Dratel and that he shares with them. Indeed, some witnesses abroad have not and will not communicate with Mr. Dratel

at all electronically, because they believe that by sharing information with him, they are also sharing information with the U.S. government. At times, Mr. Dratel must forgo these communications altogether. The cost of traveling to certain remote areas of the globe to interview a potential witness in-person can be too high to justify the travel, and some regions are simply too dangerous or inaccessible to permit in-person visits.

Human Rights Watch

130. HRW is a non-profit, non-governmental human rights organization based in New York City. It employs approximately 400 staff members located across offices around the world. Formed in 1978, HRW's mission is to defend the rights of people worldwide. HRW conducts fact-finding investigations into human rights abuses by governments and non-state actors in all regions of the world.

131. HRW engages in international and domestic internet communications that are essential to its mission. Among other things, HRW's U.S.-based staff routinely engage in sensitive and confidential internet communications with non-U.S. persons located abroad in carrying out HRW's research, reporting, and advocacy work.

132. HRW's communications are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of HRW's communications and it violates HRW's right to control those communications and the information they contain.

133. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates HRW's international communications because HRW is communicating with or about persons the government has targeted for Upstream surveillance. HRW's international contacts include foreign government officials, humanitarian agencies, think tanks, military officials, human rights defenders, politicians, dissidents, victims of human rights abuses,

perpetrators of human rights abuses, religious groups, media, and scholars, some of whom are likely targets. HRW's communications with these contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." HRW communicates both with and about these likely targets. HRW's international communications contain, among other things, details about its foreign contacts and other important sources of information—details such as the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to HRW's work.

134. Upstream surveillance undermines HRW's ability to conduct its work. HRW's research, reporting, and advocacy depend on the confidentiality of its communications, including its ability to assure its contacts that their communications—and, in some cases, even their identities—will not be revealed. Due in part to NSA surveillance, including Upstream surveillance, HRW has undertaken burdensome and costly measures to secure and protect its communications, including adopting more secure methods of electronic communication, traveling to conduct in-person meetings, and in some instances avoiding sensitive topics or forgoing communications altogether. Despite these precautions, HRW believes that Upstream surveillance reduces the likelihood that sources, witnesses, experts, foreign government officials, and victims of human rights abuses will share sensitive information with HRW's staff, because they fear that their communications will be intercepted by the U.S. government and also shared with the other governments, intelligence services, and organizations with which the U.S. government cooperates.

Amnesty International USA

135. AIUSA, headquartered in New York City, is one of Amnesty International's largest national sections, with hundreds of thousands of members and supporters. Through its

advocacy campaigns, AIUSA seeks to expose and stop human rights abuses in the United States and throughout the world.

136. AIUSA engages in international and domestic internet communications that are essential to its mission. Among other things, some of AIUSA's U.S.-based staff—as well as some AIUSA members who serve as volunteer specialists on particular countries and thematic issues—routinely engage in sensitive and confidential internet communications with non-U.S. persons located abroad in carrying out AIUSA's reporting and advocacy work.

137. AIUSA's communications are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of AIUSA's communications and it violates AIUSA's right to control those communications and the information they contain.

138. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates AIUSA's international communications because AIUSA is communicating with or about persons the government has targeted for Upstream surveillance. AIUSA's international contacts include Amnesty International researchers who are documenting and witnessing human rights violations in the field, human rights defenders, victims of violations and their families, eyewitnesses to violations, political dissidents, government officials, journalists, and lawyers, some of whom are likely targets. AIUSA's communications with these contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." AIUSA communicates both with and about these likely targets. AIUSA's international communications contain, among other things, details about its foreign contacts and other important sources of information—details such as the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to AIUSA's work.

139. Upstream surveillance undermines AIUSA's ability to conduct its work. AIUSA's reporting and advocacy depends on the confidentiality of its communications, including its ability to assure its contacts that their communications—and, in some cases, even their identities—will not be revealed. Due in part to NSA surveillance, including Upstream surveillance, some AIUSA staff strive to communicate particularly sensitive matters in-person, and must sometimes avoid sensitive topics or forgo exchanging information about these matters altogether. Despite these precautions, AIUSA believes that Upstream surveillance reduces the likelihood that sources, witnesses, experts, foreign government officials, and victims of human rights abuses will share sensitive information with AIUSA's staff and members, because they fear that their communications will be intercepted by the U.S. government and also shared with the other governments, intelligence services, and organizations with which the U.S. government cooperates.

PEN American Center

140. PEN is an association based in New York City of approximately 4,000 novelists, journalists, editors, poets, essayists, playwrights, publishers, translators, agents, and other professionals, and an even larger network of readers and supporters. It is the largest of the organizations within PEN International. For the last 90 years, PEN has worked to ensure that people all over the world are at liberty to create literature, to convey ideas freely, and to express their views unimpeded. One of PEN's core projects is to advocate on behalf of persecuted writers across the globe, so that they might be free to write and to express their ideas.

141. PEN engages in international and domestic internet communications that are essential to its mission. Among other things, PEN's U.S.-based staff routinely engage in

sensitive and confidential internet communications with non-U.S. persons located abroad in carrying out PEN's research and advocacy work.

142. PEN's communications are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of PEN's communications and it violates PEN's right to control those communications and the information they contain.

143. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates PEN's international communications because PEN is communicating with or about persons the government has targeted for Upstream surveillance. PEN's international contacts include writers whose work and experiences relate to political upheavals, human rights violations, freedom of the press, and government surveillance; those writers' families and legal representatives; human rights defenders; and other PEN partners in countries such as Syria, Cuba, China, Iran, and Ethiopia—some of whom are likely targets. PEN's communications with these contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." PEN communicates both with and about these likely targets. PEN's international communications contain, among other things, details about its foreign contacts and other important sources of information—details such as the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to PEN's work.

144. Upstream surveillance undermines PEN's ability to conduct its work. PEN's research and advocacy depend on the confidentiality of its communications, including its ability to assure its contacts that their communications—and, in some cases, even their identities—will not be revealed. Due in part to NSA surveillance, including Upstream surveillance, PEN staff have undertaken burdensome measures to secure and protect their

communications, including adopting more secure methods of electronic communication, and in some instances avoiding sensitive topics or forgoing communications altogether. Despite these precautions, PEN believes that Upstream surveillance reduces the likelihood that foreign writers and other contacts will share sensitive information with PEN's staff, because they fear that their communications will be intercepted by the U.S. government and also shared with the other governments, intelligence services, and organizations with which the U.S. government cooperates.

Global Fund for Women

145. GFW, based in San Francisco and New York City, is a grant-maker and a global advocate for women's human rights. GFW advances the movement for women's human rights by directing resources to and raising the voices of women worldwide. GFW invests in local, courageous women and women-led organizations, and creates digital advocacy campaigns on critical global issues for women and girls. Since its inception in 1986, GFW has awarded 9,921 grants totaling $120 million to 4,759 organizations in 175 countries.

146. GFW engages in international and domestic internet communications that are essential to its mission. Among other things, GFW's U.S.-based staff routinely engage in sensitive, confidential, and privileged internet communications with non-U.S. persons located abroad in carrying out GFW's grant-making and advocacy work.

147. GFW's communications are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of GFW's communications and it violates GFW's right to control those communications and the information they contain.

148. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates GFW's international communications because GFW is communicating with or

about persons the government has targeted for Upstream surveillance. GFW's international contacts include foreign banks, foreign government agencies, funders, attorneys, and grantee and partner organizations working in conflict zones or on politically sensitive issues abroad, some of whom are likely targets. GFW's communications with these contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." GFW communicates both with and about these likely targets. GFW's international communications contain, among other things, details about its foreign contacts and other important sources of information—details such as the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to GFW's work.

149. Upstream surveillance undermines GFW's ability to conduct its work. GFW's grant-making depends on the confidentiality of its communications, including its ability to assure its contacts that their communications—and, in some cases, even their identities—will not be revealed. Due in part to NSA surveillance, including Upstream surveillance, GFW's staff must exercise extreme caution when engaging in certain international communications, and in some instances avoid sensitive topics or forgo communications altogether. Some of GFW's international contacts will communicate with the organization only by phone or Skype, rather than email, because they believe that email is a less secure means of communication. Other of GFW's international contacts will communicate via email, but only if staff avoid using certain words in their communications that may result in further government scrutiny. Despite these precautions, GFW believes that Upstream surveillance reduces the likelihood that current and prospective grantees will share sensitive information with GFW's staff, because they fear that their communications will be intercepted by the U.S. government and also shared with the

other governments, intelligence services, and organizations with which the U.S. government cooperates.

The Nation Magazine

150. The Nation is America's oldest weekly magazine of opinion, news, and culture. The Nation is also a digital media company, reporting daily on politics, social issues, and the arts. Its journalists report on a wide range of issues relating to international affairs, including the wars in Iraq and Afghanistan, the Israel–Palestine conflict, protest activities and politics in China and elsewhere in East Asia, and civil wars and other conflicts in Africa and Latin America.

151. The Nation engages in international and domestic internet communications that are essential to its mission. Among other things, The Nation's staff and contributing writers routinely engage in sensitive and confidential internet communications with non-U.S. persons located abroad in carrying out The Nation's research, reporting, and editing.

152. The Nation's communications are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of The Nation's communications and it violates The Nation's right to control those communications and the information they contain.

153. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates The Nation's international communications because The Nation is communicating with or about persons the government has targeted for Upstream surveillance. The Nation's international contacts include foreign journalists in conflict zones, foreign government officials, political dissidents, human rights activists, and members of guerrilla and insurgency movements, some of whom are likely targets. The Nation's communications with these

contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." The Nation communicates both with and about these likely targets. The Nation's international communications contain, among other things, details about its foreign contacts and other important sources of information—details such as the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to The Nation's work.

154. Upstream surveillance undermines The Nation's ability to conduct its work. The Nation's research and reporting depends on the confidentiality of its communications, including its ability to assure its contacts that their communications—and, in some cases, even their identities—will not be revealed. Due in part to NSA surveillance, including Upstream surveillance, The Nation has undertaken burdensome and costly measures to protect its communications, including adopting more secure methods of electronic communication, and in some instances avoiding sensitive topics or forgoing communications altogether. Despite these precautions, The Nation believes that Upstream surveillance reduces the likelihood that foreign journalists and sources will share sensitive information with The Nation, because they fear that their communications will be intercepted by the U.S. government and also shared with the other governments, intelligence services, and organizations with which the U.S. government cooperates.

The Rutherford Institute

155. The Rutherford Institute, founded in 1982 and based in Virginia, is a civil liberties organization committed to protecting the constitutional freedoms of Americans and the human rights of all people. Rutherford provides free legal services in defense of civil liberties

and educates the public about constitutional and human rights issues. It also advocates on behalf of individuals abroad whose rights are threatened by foreign governments.

156. Rutherford engages in international and domestic internet communications that are essential to its mission. Among other things, Rutherford's staff, who are based in the U.S., routinely engage in sensitive and confidential internet communications with non-U.S. persons located abroad in carrying out Rutherford's advocacy, legal, and educational activities.

157. Rutherford's communications are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of Rutherford's communications, and it violates Rutherford's right to control those communications and the information they contain.

158. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates Rutherford's international communications because Rutherford is communicating with or about persons the government has targeted for Upstream surveillance. Rutherford's international contacts include human rights and civil liberties advocates, foreign government officials, and individuals whose rights are threatened by the U.S. or foreign governments, some of whom are likely targets. Rutherford's communications with these contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." Rutherford communicates both with and about these likely targets. Rutherford's international communications, among other things, contain details about its foreign contacts and other important sources of information—details such as the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to Rutherford's work.

159. Upstream surveillance undermines Rutherford's ability to conduct its work. Rutherford's advocacy depends on its ability to assure its contacts that their communications—and, in some cases, even their identities—will not be revealed. Due in part to NSA surveillance, including Upstream surveillance, Rutherford in some instances avoids sensitive topics or forgoes communications altogether. Rutherford believes that Upstream surveillance reduces the likelihood that victims of human rights abuses, witnesses, foreign government officials, and other contacts will share sensitive information with Rutherford, because they fear that their communications will be intercepted by the U.S. government and also shared with the other governments, intelligence services, and organizations with which the U.S. government cooperates.

The Washington Office on Latin America

160. WOLA is a non-profit, non-governmental organization based in Washington D.C. WOLA works to advance human rights and social justice in the Americas. WOLA is regularly called upon for its research and analysis by policymakers, the media, and academics in the U.S. and Latin America. To further this work, WOLA gathers and publishes information about U.S. policies concerning Latin America, U.S. assistance (military or otherwise) to Latin American countries, and U.S. immigration practices, among other things.

161. WOLA engages in international and domestic internet communications that are essential to its mission. Among other things, WOLA's U.S.-based staff routinely engage in sensitive and confidential internet communications with non-U.S. persons located abroad in carrying out WOLA's research, policy, and advocacy work.

162. WOLA's communications are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of WOLA's communications and it violates WOLA's right to control those communications and the information they contain.

163. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates WOLA's international communications because WOLA is communicating with or about persons the government has targeted for Upstream surveillance. For instance, WOLA communicates with foreign government officials located abroad—including at times presidents and foreign ministers. Similarly, it communicates with policymakers, academics, journalists, human rights defenders, victims of human rights abuses, and staff from multilateral institutions, such as the Organization of American States, the Inter-American Development Bank, and the United Nations, some of whom are also likely targets. WOLA's communications with these contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." WOLA communicates both with and about these likely targets. WOLA's international communications contain, among other things, details about its foreign contacts and other important sources of information—details such as the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to WOLA's work.

164. Upstream surveillance undermines WOLA's ability to conduct its work. WOLA's research and advocacy depend on the confidentiality of its communications, including its ability to assure its contacts that their communications—and, in some cases, even their identities—will not be revealed. Due in part to NSA surveillance, including Upstream surveillance, WOLA has undertaken burdensome and costly measures to secure and protect its communications, including adopting more secure methods of electronic communication,

traveling to conduct in-person meetings, and in some instances avoiding sensitive topics or forgoing communications altogether. Despite these precautions, WOLA believes that Upstream surveillance reduces the likelihood that policymakers, foreign government officials, experts, witnesses, and victims of human rights abuses will share sensitive information with WOLA's staff, because they fear that their communications will be intercepted by the U.S. government and also shared with the other governments, intelligence services, and organizations with which the U.S. government cooperates.

CAUSES OF ACTION

165. Upstream surveillance exceeds the authority granted by 50 U.S.C. § 1881a, and therefore violates 5 U.S.C. § 706.

166. Upstream surveillance violates the Fourth Amendment to the Constitution.

167. Upstream surveillance violates the First Amendment to the Constitution.

168. Upstream surveillance violates Article III of the Constitution.

PRAYER FOR RELIEF

WHEREFORE Plaintiffs respectfully request that the Court:

1. Exercise jurisdiction over Plaintiffs' Complaint;

2. Declare that Upstream surveillance violates 50 U.S.C. § 1881a and 5 U.S.C. § 706;

3. Declare that Upstream surveillance is unconstitutional under the First and Fourth Amendments, and under Article III;

4. Permanently enjoin Defendants from continuing Upstream surveillance;

5. Order Defendants to purge all records of Plaintiffs' communications in their possession obtained pursuant to Upstream surveillance;

6. Award Plaintiffs fees and costs pursuant to 28 U.S.C. § 2412;

7. Grant such other and further relief as the Court deems just and proper.

Dated: June 19, 2015
Baltimore, Maryland

Respectfully submitted,

/s/ Deborah A. Jeon
Deborah A. Jeon
(Bar No. 06905)
jeon@aclu-md.org
David R. Rocah
(Bar No. 27315)
rocah@aclu-md.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF MARYLAND
3600 Clipper Mill Rd., #350
Baltimore, MD 21211
Phone: (410) 889-8555
Fax: (410) 366-7838

/s/ Patrick Toomey
Patrick Toomey
(pro hac vice)
ptoomey@aclu.org
(*signed by Patrick Toomey with permission of Debbie A. Jeon*)
Jameel Jaffer
(pro hac vice)
jjaffer@aclu.org
Alex Abdo
(pro hac vice)
aabdo@aclu.org
Ashley Gorski
(pro hac vice)
agorski@aclu.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654

Charles S. Sims
(pro hac vice)

csims@proskauer.com
David A. Munkittrick
(pro hac vice)
dmunkittrick@proskauer.com
John M. Browning
(pro hac vice)
jbrowning@proskauer.com
PROSKAUER ROSE LLP
Eleven Times Square
New York, NY 10036
Phone: (212) 969-3000
Fax: (212) 969-2900

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION,

Plaintiff,

v.

NATIONAL SECURITY AGENCY / CENTRAL SECURITY SERVICE, *et al.*,

Defendants.

Hon. T. S. Ellis, III

Civil Action No.
15-cv-00662-TSE

DECLARATION OF PATRICK TOOMEY IN SUPPORT OF PLAINTIFF WIKIMEDIA FOUNDATION'S MOTION TO COMPEL

I, Patrick Toomey, a member of the Bar of the State of New York and admitted *pro hac vice* to the Bar of this Court, declare under penalty of perjury as follows:

1. I am an attorney with the American Civil Liberties Union Foundation, and represent Plaintiff Wikimedia Foundation ("Wikimedia") in this matter. I submit this declaration in support of Plaintiff's Motion to Compel.

2. Attached hereto as **Exhibit 1** is a chart identifying Plaintiff's Requests for Admission, Interrogatories, and Requests for Production, as modified by Wikimedia following the parties' meet-and-confer discussions, that are at issue in this Motion to Compel.

3. Attached hereto as **Exhibit 2** is a true and correct copy of Plaintiff's First Set of Requests for Admission.

4. Attached hereto as **Exhibit 3** is a true and correct copy of Plaintiff's Second Set of Requests for Admission.

5. Attached hereto as **Exhibit 4** is a true and correct copy of Plaintiff's Third Set of Requests for Admission.

6. Attached hereto as **Exhibit 5** is true and correct copy of Plaintiff's First Set of Interrogatories.

7. Attached hereto as **Exhibit 6** is a true and correct copy of Plaintiff's Second Set of Interrogatories.

8. Attached hereto as **Exhibit 7** is a true and correct copy of Plaintiff's First Set of Requests for Production.

9. Attached hereto as **Exhibit 8** is a true and correct copy of Plaintiff's Second Set of Requests for Production.

10. Attached hereto as **Exhibit 9** is a true and correct copy of Defendant National Security Agency's ("NSA") Objections and Responses to Plaintiff's First and Second Sets of Requests for Admission.

11. Attached hereto as **Exhibit 10** is a true and correct copy of Defendant NSA's Objections to Plaintiff's Third Set of Requests for Admission.

12. Attached hereto as **Exhibit 11** is a true and correct copy of Defendant NSA's Objections and Responses to Plaintiff's First Set of Interrogatories.

13. Attached hereto as **Exhibit 12** is a true and correct copy of Defendant NSA's Objections to Plaintiff's Second Set of Interrogatories.

14. Attached hereto as **Exhibit 13** is a true and correct copy of Defendant NSA's Objections and Responses to Plaintiff's First and Second Sets of Requests for Production.

15. Attached hereto as **Exhibit 14** is a true and correct copy of Defendant Department of Justice's ("DOJ") Objections and Responses to Plaintiff's First and Second Sets of Requests for Admission.

16. Attached hereto as **Exhibit 15** is a true and correct copy of Defendant DOJ's Objections and Responses to Plaintiff's First Set of Interrogatories.

17. Attached hereto as **Exhibit 16** is a true and correct copy of Defendant DOJ's Objections and Responses to Plaintiff's First and Second Sets of Requests for Production.

18. Attached hereto as **Exhibit 17** is a true and correct copy of Defendant Office of the Director of National Intelligence's ("ODNI") Objections and Responses to Plaintiff's First and Second Sets of Requests for Admission.

19. Attached hereto as **Exhibit 18** is a true and correct copy of Defendant ODNI's Objections and Responses to Plaintiff's First Set of Interrogatories.

20. Attached hereto as **Exhibit 19** is a true and correct copy of Defendant ODNI's Revised Objections and Responses to Plaintiff's First and Second Sets of Requests for Production.

21. Attached hereto as **Exhibit 20** is a true and correct copy of Defendant NSA's Privilege Log.

22. Attached hereto as **Exhibit 21** is a true and correct copy of Defendant DOJ's Privilege Log.

23. Attached hereto as **Exhibit 22** is a true and correct copy of Defendant ODNI's Privilege Log.

24. Attached hereto as **Exhibit 23** is a true and correct copy of Plaintiff's Notice of Deposition Pursuant to Federal Rule of Civil Procedure 30(b)(6).

25. Attached hereto as **Exhibit 24** is a true and correct copy of a letter from James Gilligan, counsel for Defendant NSA, to Patrick Toomey, counsel for Plaintiff Wikimedia, regarding Defendant NSA's objections to Plaintiff's notice of deposition pursuant to Federal Rule of Civil Procedure 30(b)(6), dated March 22, 2018.

26. Attached hereto as **Exhibit 25** is a true and correct copy of a redacted FISC submission titled "Government's Response to the Court's Briefing Order of May 9, 2011," dated June 1, 2011, and labeled with Bates numbers NSA-WIKI 00234–77 ("June 1, 2011 FISC Submission"). It is available at: https://www.dni.gov/files/documents/icotr/NYT/Government's%20Response%20to%20May%209,%202011%20Briefing%20Order%20(June%201,%202011).pdf.

27. Attached hereto as **Exhibit 26** is a true and correct copy of a redacted FISC submission titled "Government's Response to the Court's Follow-Up Questions of June 17, 2011," dated June 28, 2011, and publicly released pursuant to the Freedom of Information Act ("June 28, 2011 FISC Submission"). It is available at: https://www.documentcloud.org/documents/4064819-Savage-NYT-FOIA-2011-Bates-MCT-third-tranche.html#document/p176.[1]

28. Attached hereto as **Exhibit 27** is a true and correct copy of a redacted FISC Memorandum Opinion, dated October 3, 2011, and labeled with Bates numbers NSA-WIKI 00149–229. It is available at: https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf.

29. Attached hereto as **Exhibit 28** is a true and correct copy of a redacted FISC Memorandum Opinion, dated September 20, 2012, and publicly released pursuant to the

[1] Although Defendants have stated that FISC opinions and FISC submissions released via FOIA are readily accessible at "various locations" on Defendant ODNI's public website, *see, e.g.*, NSA Resp. to Pl. Requests for Production No. 21, Plaintiff has been unable to locate a functioning web-link to this document and others on ODNI's website.

Freedom of Information Act. It is available at: https://www.aclu.org/sites/default/files/field_document/fisc-opinion-and-order-re-1809-dated09.20.2012-ocrd_2.pdf.

30. Attached hereto as **Exhibit 29** is a true and correct copy of a redacted FISC Memorandum Opinion and Order, dated April 26, 2017. It is available at: https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf.

31. Attached hereto as **Exhibit 30** is a true and correct copy of a document titled "Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended," dated July 25, 2014. It is available at: https://www.dni.gov/files/documents/icotr/702/Bates%20365-373.pdf .

* * *

I declare under penalty of perjury that the foregoing is true and correct.

Patrick Toomey

Date: March 26, 2018
New York, New York

Exhibit 1

Wikimedia Foundation v. National Security Agency, et. al.
No. 15-cv-00662-TSE

Plaintiff Wikimedia's Discovery Requests at Issue, as Narrowed by Plaintiff

DEFINITIONS

Notwithstanding any definition set forth below, each word, term, or phrase used in [each] Request is intended to have the broadest meaning permitted under the Federal Rules of Civil Procedure. As used in [each] Request, the following terms are to be interpreted in accordance with these definitions:

Answer: The term "ANSWER" means Defendants' Answer to Plaintiff's First Amended Complaint in this action, filed on October 16, 2017.

Bulk: To COPY or REVIEW INTERNET COMMUNICATIONS in "BULK" means to COPY or REVIEW INTERNET COMMUNICATIONS in large quantity without prior application of SELECTORS, or other identifiers associated with specific targets of Upstream surveillance.

Circuit: The term "CIRCUIT" has the ordinary meaning of that term within the telecommunications industry as understood by YOU in the context of Upstream surveillance.

Communication: The term "COMMUNICATION" means information transmitted by any means, whether orally, electronically, by document, or otherwise.

Concern or Concerning: The terms "CONCERN" and "CONCERNING" mean relating to, referring to, describing, evidencing, constituting, reflecting, memorializing, identifying, embodying, pertaining to, commenting on, discussing, analyzing, considering, containing, consisting of, indicating, supporting, refuting, or connected to.

Copy: The term "COPY" means to duplicate a piece of data (for any duration, no matter how brief).

Describe: The term "DESCRIBE" means to provide a narrative statement or description of the specific facts or matters to which an Interrogatory refers, including, but not limited to, an identification of all persons, communications, acts, transactions, events, agreements, recommendations, and DOCUMENTS used, necessary, or desirable to support such statement or make the description complete.

Document: The term "DOCUMENT" shall have the broadest meaning ascribed to that term in Federal Rule of Civil Procedure 34 and Federal Rule of Evidence 1001. The term also includes any parent or child attachment or other documents embedded or linked in any way to a requested document. A draft or non-identical copy is a separate document within the meaning of the term "DOCUMENT."

Identify (with respect to PERSONS): When referring to a PERSON, to "IDENTIFY" means to state the PERSON's full name, present or last known address, and, when referring to a natural person, the present or last known place of employment. If the business and home telephone numbers are known to the answering party, and if the PERSON is not a party or present employee of a party, said telephone numbers shall be provided. Once a PERSON has been identified in accordance with this subparagraph, only the name of the PERSON need be listed in response to subsequent discovery requesting the identification of that PERSON.

Identify (with respect to documents): When referring to documents, to "IDENTIFY" means to state the: (i) type of document; (ii) general subject matter; (iii) date of the document; and (iv) author(s), addressee(s), and recipient(s); or, alternatively, to produce the document.

Interacted With **[as modified]**: The term "INTERACTED WITH" means to have used a device to COPY, filter, or REVIEW an INTERNET COMMUNICATION or INTERNET TRANSACTION while such communication or transaction is being transmitted or while the communication or transaction is being stored, other than as necessary to transmit or store the communication or transaction in the ordinary course of its transmission or storage.

International Communication: The term "INTERNATIONAL COMMUNICATION" means an INTERNET COMMUNICATION between at least one party in the UNITED STATES and at least one party outside the UNITED STATES.

Internet Backbone: The term "INTERNET BACKBONE" means the set of high capacity cables, switches, and routers that facilitates both domestic and international Internet communication by parties connected to it. The INTERNET BACKBONE includes, but is not limited to, the international submarine cables that carry INTERNET COMMUNICATIONS.

Internet Communication: The term "INTERNET COMMUNICATION" means a series of related packets that are sent from a particular source to a particular destination that together constitute a message of some sort, including but not limited to an email message, an HTTP request, or an HTTP response.

Internet Packet: The term "INTERNET PACKET" means a discrete chunk of information transmitted across the Internet. All INTERNET COMMUNICATIONS are split into one or more INTERNET PACKETS. Each INTERNET PACKET contains a source and destination Internet Protocol ("IP") address and some payload.

Internet Transaction: The term "INTERNET TRANSACTION" has the same meaning as "Internet transaction" within the PCLOB Report at pages 39 and 125 and note 517.

NSA: The terms "National Security Agency" and "NSA" include any department, office, entity, officer, employee, agent, representative, attorney, consultant, or contractor thereof, as well as telecommunication providers acting at the NSA's direction.

Parties: The terms "PLAINTIFF" and "DEFENDANT," as well as a party's full or abbreviated name or a pronoun referring to a party, mean that party and its officers, directors,

employees, agents, representatives, attorneys, consultants, and contractors. This definition is not intended to impose a discovery obligation on any PERSON who is not a party to the litigation or to limit the Court's jurisdiction to enter any appropriate order.

Person: The term "PERSON" is defined as any natural person or any business, legal or governmental entity, or association.

Process: The term "PROCESS" has the same meaning as "process," "process[ed]," or "process[ing]" within the July 2014 Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended, *available at* https://www.dni.gov/files/documents/0928/2014%20NSA%20702%20Minimization%20Procedures.pdf ("2014 NSA Minimization Procedures").

Retain: The term "RETAIN" has the same meaning as "retain," "retained," or "retention" within the 2014 NSA Minimization Procedures.

Review **[as modified]**: The term "REVIEW" means to examine, scan, screen, monitor, analyze, or gather information about the contents of.

Selector: The term "SELECTOR" has the same meaning as "selector" within the 2014 NSA Minimization Procedures.

Target: The term "TARGET" means the subjects who are "targeted" pursuant to 50 U.S.C. § 1881a.

United States: When used as a term of geographic location, "UNITED STATES" means all areas under the territorial sovereignty of the United States.

Wholly Domestic Communication: The term "WHOLLY DOMESTIC COMMUNICATION" means an INTERNET COMMUNICATION whose origin and final destination are both located within the UNITED STATES.

You/Your: The terms "YOU" or "YOUR" include the defendant agency, and department, office, entity, officer, employee, agent, representative, attorney, consultant, or contractor thereof.

The present tense includes the past and future tenses. The singular includes the plural, and the plural includes the singular. "All" means "any and all"; "any" means "any and all." "Including" means "including but not limited to." "And" and "or" encompass both "and" and "or." Words in the masculine, feminine, or neutral form shall include each of the other genders.

REQUESTS AT ISSUE

No.	Request	Modified Request
Requests for Admission		
RFA 6	Admit that, in conducting Upstream surveillance, the NSA REVIEWS the contents of INTERNET COMMUNICATIONS that are in transit on the INTERNET BACKBONE, prior to RETAINING INTERNET COMMUNICATIONS that contain a SELECTOR.	
RFA 7	Admit that, in conducting Upstream surveillance, the NSA COPIES INTERNET COMMUNICATIONS in BULK that are in transit on the INTERNET BACKBONE.	
RFA 8	Admit that, in conducting Upstream surveillance, the NSA REVIEWS the contents of INTERNET COMMUNICATIONS in BULK that are in transit on the INTERNET BACKBONE.	
RFA 9	Admit that, in conducting Upstream surveillance, the NSA COPIES INTERNET COMMUNICATIONS that are neither to nor from TARGETS, prior to RETAINING INTERNET COMMUNICATIONS that contain a SELECTOR.	
RFA 10	Admit that, in conducting Upstream surveillance, the NSA REVIEWS the contents of INTERNET COMMUNICATIONS that are neither to nor from TARGETS, prior to RETAINING INTERNET COMMUNICATIONS that contain a SELECTOR.	

No.	Request	Modified Request
RFA 13	Admit that the NSA conducts Upstream surveillance on multiple INTERNET BACKBONE CIRCUITS.	
RFA 14	Admit that the NSA conducts Upstream surveillance on multiple "international Internet link[s]," as that term is used by the government in its submission to the Foreign Intelligence Surveillance Court, titled "Government's Response to the Court's Briefing Order of May 9, 2011," and filed on June 1, 2011, *see* [*Redacted*], 2011 WL 10945618, at *15 (FISC Oct. 3, 2011).	Admit that the NSA conducts Upstream surveillance on multiple "international Internet link[s]," as that term is used by the Foreign Intelligence Surveillance Court in describing Upstream surveillance, *see* [*Redacted*], 2011 WL 10945618, at *15 (FISC Oct. 3, 2011).
RFA 15	Admit that the NSA conducts Upstream surveillance at multiple INTERNET BACKBONE "chokepoints" or "choke points" (as that term is used by YOU).	Admit that the NSA conducts Upstream surveillance at multiple INTERNET BACKBONE "chokepoints" or "choke points."
RFA 16	Admit that the document attached hereto as Exhibit A, titled "Why are we interested in HTTP?," is a true and correct excerpted copy of a genuine document.	Admit that the document attached hereto as Exhibit A, titled "Why are we interested in HTTP?," is a true and correct excerpted copy of a genuine NSA document.
RFA 17	Admit that the statements within the document attached hereto as Exhibit A were made by YOUR employees on matters within the scope of their employment during the course of their employment.	
RFA 18	Admit that statements within the document attached hereto as Exhibit A were made by persons YOU authorized to make statements on the subjects of the statements within the document.	
RFA 19	Admit that the document attached hereto as Exhibit B, titled "Fingerprints and Appids," and "Fingerprints and Appids (more)," is a true and correct excerpted copy of a genuine document.	Admit that the document attached hereto as Exhibit B, titled "Fingerprints and Appids," and "Fingerprints and Appids (more)," is a true and correct excerpted copy of a genuine NSA document.

No.	Request	Modified Request
RFA 20	Admit that the statements within the document attached hereto as Exhibit B were made by YOUR employees on matters within the scope of their employment during the course of their employment.	
RFA 21	Admit that statements within the document attached hereto as Exhibit B were made by persons YOU authorized to make statements on the subjects of the statements within the document.	
RFA 25	Admit that the document attached hereto as Exhibit D, titled "SSO's Support to the FBI for Implementation of their Cyber FISA Orders," is a true and correct copy of a genuine document.	Admit that the document attached hereto as Exhibit D, titled "SSO's Support to the FBI for Implementation of their Cyber FISA Orders," is a true and correct copy of a genuine NSA document.
RFA 26	Admit that the statements within the document attached hereto as Exhibit D were made by YOUR employees on matters within the scope of their employment during the course of their employment.	
RFA 27	Admit that statements within the document attached hereto as Exhibit D were made by persons YOU authorized to make statements on the subjects of the statements within the document.	
RFA 28	Admit that the document attached hereto as Exhibit E, titled "Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended" and dated July 28, 2009 (the "NSA Targeting Procedures") is a true and correct copy of a genuine document.	Admit that the document attached hereto as Exhibit E, titled "Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended" and dated July 28, 2009 (the "NSA Targeting Procedures") is a true and correct copy of a genuine DOJ document.

No.	Request	Modified Request
RFA 29	Admit that the statements within the document attached hereto as Exhibit E were made by YOUR employees on matters within the scope of their employment during the course of their employment.	
RFA 30	Admit that statements within the document attached hereto as Exhibit E were made by persons YOU authorized to make statements on the subjects of the statements within the document.	
RFA 34	Admit that, in conducting Upstream surveillance, the NSA has COPIED at least one WIKIMEDIA INTERNET COMMUNICATION.	
RFA 35	Admit that, in conducting Upstream surveillance, the NSA has REVIEWED the content of at least one WIKIMEDIA INTERNET COMMUNICATION.	
RFA 36	Admit that, in conducting Upstream surveillance, the NSA has RETAINED at least one WIKIMEDIA INTERNET COMMUNICATION.	
RFA 37	Admit that, in conducting Upstream surveillance on or before June 22, 2015, the NSA screened the contents of Internet web traffic (that is, the application layer of HTTP and HTTPS communications).	
RFA 38	Admit that, in conducting Upstream surveillance as of the date of the service of this request, the NSA screens the contents of Internet web traffic (that is, the application layer of HTTP and HTTPS communications).	

No.	Request	Modified Request
RFA 39	Admit that the document attached hereto as Exhibit A, which describes the monitoring of hundreds of CIRCUITS at one international cable site, is a true and correct excerpted copy of a genuine NSA document.	
RFA 40	If YOU contend, for the purpose of contesting jurisdiction in this matter, that encryption bears in any way on the interception, accessing, COPYING, filtering, REVIEWING, ingestion, or RETENTION of WIKIMEDIA'S COMMUNICATIONS in the course of Upstream surveillance, admit that YOU have the ability to decrypt, decipher, or render intelligible the contents of some HTTPS communications subject to Upstream surveillance.	
Interrogatories		
ROG 1	DESCRIBE YOUR understanding of the definition of the term "international Internet link" as used by the government in its submission to the Foreign Intelligence Surveillance Court— titled "Government's Response to the Court's Briefing Order of May 9, 2011," and filed on June 1, 2011, *see [Redacted]*, 2011 WL 10945618, at *15 (FISC Oct. 3, 2011)—and provide all information supporting that understanding.	DESCRIBE YOUR understanding of the definition of the term "international Internet link" as used by the Foreign Intelligence Surveillance Court in describing Upstream surveillance, *see [Redacted]*, 2011 WL 10945618, at *15 (FISC Oct. 3, 2011), and provide all information supporting that understanding.

No.	Request	Modified Request
ROG 2	DESCRIBE YOUR understanding of the definition of the term "circuit" as used at pages 36 to 37 of the PCLOB Report, and provide all information supporting that understanding, including but not limited to all information furnished by DEFENDANTS to the Privacy and Civil Liberties Oversight Board concerning this term.	
ROG 3	DESCRIBE YOUR understanding of the definition of the term "filtering mechanism" as used at pages 10 and 47–48 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.	
ROG 4	DESCRIBE YOUR understanding of the definition of the term "scanned" as used at page 10 of the Memorandum in Support of Defendants' Motion to Dismiss the First Amended Complaint, *Wikimedia Foundation v. NSA*, No. 15-cv-662-TSE (D. Md. Aug. 6, 2015), and provide all information supporting that understanding.	
ROG 5	DESCRIBE YOUR understanding of the definition of the term "screen" as used at page 48 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.	
ROG 6	DESCRIBE YOUR understanding of the definition of the term "discrete communication" as used in the 2014 NSA Minimization Procedures, and provide all information supporting that understanding.	

No.	Request	Modified Request
ROG 7	DESCRIBE YOUR understanding of all features that a series of INTERNET PACKETS comprising an "Internet transaction" has in common, as the term "Internet transaction" is used in at page 10 n.3 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding. For example, the INTERNET PACKETS comprising an "Internet transaction" might share source and destination IP addresses, source and destination ports, and protocol type (albeit with the source and destination IP addresses and ports reversed for packets flowing in the opposite direction).	
ROG 8	DESCRIBE YOUR understanding of the definitions of the terms "single communication transaction" and "multi-communication transaction" as used by the government in its submission to the Foreign Intelligence Surveillance Court, filed on August 16, 2011, and provide all information supporting that understanding. *See* [*Redacted*], 2011 WL 10945618, at *9 (FISC Oct. 3, 2011).	
ROG 9	DESCRIBE YOUR understanding of the definitions of the terms "access" and "larger body of international communications" as used at page 10 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.	

No.	Request	Modified Request
ROG 14	DESCRIBE the entire process by which, pursuant to Upstream surveillance, the contents of INTERNET COMMUNICATIONS are INTERACTED WITH.	
ROG 15	DESCRIBE any and all statements or facts YOU contend are inaccurate concerning Upstream surveillance in pages 7-10, 22, 32-33, 35-41 & n.157, 79, 111 n.476, 119-26, and 143-45 of the Privacy and Civil Liberties Oversight Board's *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (July 2, 2014), based on Upstream surveillance as it was conducted on the date the report was publicly released.	
ROG 16	DESCRIBE the approximate percentage of CIRCUITS carrying Internet communications into or out of the United States (not CIRCUITS carrying solely telephonic or private network communications) that were monitored in the course of Upstream surveillance in each of the years 2015, 2016, and 2017. If insufficient information is available for these three years, please provide sufficient information for the three most recent years available.	

No.	Request	Modified Request
ROG 17	DESCRIBE the approximate percentage of international submarine cables carrying Internet communications into or out of the United States (not international submarine cables carrying solely telephonic or private network communications) that were monitored in the course of Upstream surveillance in each of the years 2015, 2016, and 2017. If insufficient information is available for these three years, please provide sufficient information for the three most recent years available.	
ROG 18	DESCRIBE, by any metric commonly used in the telecommunications industry, such as bytes or packets, the approximate amount of Internet traffic that was subject to filtering in the course of Upstream surveillance, prior to retaining Internet communications that contain a selector, in each of the years 2015, 2016, and 2017. If insufficient information is available for these three years, please provide sufficient information for the three most recent years available.	
ROG 19	DESCRIBE, by any metric commonly used in the telecommunications industry, such as bytes or packets, the approximate amount of Internet traffic that was screened in the course of Upstream surveillance, prior to retaining Internet communications that contain a selector, in each of the years 2015, 2016, and 2017. If insufficient information is available for these three years, please provide sufficient information for the three most recent years available.	

No.	Request	Modified Request
ROG 20	If YOU contend, for the purpose of contesting jurisdiction in this matter, that encryption bears in any way on the interception, accessing, COPYING, filtering, REVIEWING, ingestion, or RETENTION of WIKIMEDIA'S COMMUNICATIONS in the course of Upstream surveillance, DESCRIBE the protocols used to encrypt INTERNET COMMUNICATIONS or INTERNET TRANSACTIONS subject to Upstream surveillance for which the NSA has the ability to decrypt, decipher, or render intelligible the contents of those COMMUNICATIONS.	
Requests for Production		
RFP 10	DOCUMENTS sufficient to show or estimate the number of INTERNET COMMUNICATIONS and/or INTERNET TRANSACTIONS RETAINED using Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.	
RFP 13	DOCUMENTS sufficient to show or estimate the number of CIRCUITS on which the NSA conducted Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.	
RFP 14	DOCUMENTS sufficient to show or estimate the combined bandwidth of the CIRCUITS on which the NSA conducted Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.	

No.	Request	Modified Request
RFP 15	DOCUMENTS sufficient to show or estimate the number of "international Internet link[s]"— as that term was used by the government in its submission to the Foreign Intelligence Surveillance Court, titled "Government's Response to the Court's Briefing Order of May 9, 2011," and filed on June 1, 2011, *see [Redacted]*, 2011 WL10945618, at *15 (FISC Oct. 3, 2011)—monitored using Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017.	
RFP 16	DOCUMENTS sufficient to show or estimate the number of Internet "chokepoints" or "choke points" (as that term is used by YOU) inside the UNITED STATES through which INTERNATIONAL COMMUNICATIONS enter and leave the UNITED STATES and where the NSA has established Upstream surveillance collection or PROCESSING capabilities.	
RFP 18	All Foreign Intelligence Surveillance Court–approved targeting procedures relevant at any time to DEFENDANTS' implementation of Upstream surveillance.	Foreign Intelligence Surveillance Court-approved targeting procedures relevant to DEFENDANTS' implementation of Upstream surveillance in 2009, 2015, 2016, and 2017.

No.	Request	Modified Request
RFP 21	All Foreign Intelligence Surveillance Court, Foreign Intelligence Surveillance Court of Review, and Supreme Court orders and opinions CONCERNING Upstream surveillance.	All Foreign Intelligence Surveillance Court, Foreign Intelligence Surveillance Court of Review, and Supreme Court orders and opinions CONCERNING Upstream surveillance that: a. Describe the ways in which the NSA intercepts, COPIES, filters, or REVIEWS INTERNET COMMUNICATIONS or INTERNET TRANSACTIONS in the course of Upstream surveillance in order to identify COMMUNICATIONS associated with its SELECTORS; b. Describe the points or places at which Upstream surveillance is conducted in relation to the Internet backbone and its components, including but not limited to CIRCUITS, links, or chokepoints; or c. Describe the types or categories of INTERNET COMMUNICATIONS subject to Upstream surveillance, including but not limited to COMMUNICATIONS associated with web activity or email.

No.	Request	Modified Request
RFP 22	All Foreign Intelligence Surveillance Court, Foreign Intelligence Surveillance Court of Review, and Supreme Court submissions CONCERNING Upstream surveillance.	All Foreign Intelligence Surveillance Court, Foreign Intelligence Surveillance Court of Review, and Supreme Court submissions CONCERNING Upstream surveillance that: a. Describe the ways in which the NSA intercepts, COPIES, filters, or REVIEWS INTERNET COMMUNICATIONS or INTERNET TRANSACTIONS in the course of Upstream surveillance in order to identify COMMUNICATIONS associated with its SELECTORS; b. Describe the points or places at which Upstream surveillance is conducted in relation to the Internet backbone and its components, including but not limited to CIRCUITS, links, or chokepoints; or c. Describe the types or categories of INTERNET COMMUNICATIONS subject to Upstream surveillance, including but not limited to COMMUNICATIONS associated with web activity or email.
RFP 23	Any INTERNET COMMUNICATION of WIKIMEDIA that any DEFENDANT INTERACTED WITH in connection with Upstream surveillance.	
RFP 24	All DOCUMENTS CONCERNING any INTERACTION WITH the INTERNET COMMUNICATIONS of WIKIMEDIA in connection with Upstream surveillance.	

Exhibit 2

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION,	*	
Plaintiff,	*	
v.	*	**Civil Action No.: 15-cv-00662-TSE**
NATIONAL SECURITY AGENCY, *et al.*,	*	
Defendants.	*	

* * * * * * * * * * *

REQUESTS FOR ADMISSION

Pursuant to Federal Rule of Civil Procedure 36, Local Rule 104, and Appendix A to the Local Rules, the Wikimedia Foundation ("WIKIMEDIA" or "PLAINTIFF"), by its undersigned attorneys, serves these Requests for Admission on defendants National Security Agency ("NSA"); the Office of the Director of National Intelligence ("ODNI"); the United States Department of Justice ("DOJ"); Admiral Michael S. Rogers, in his official capacity as the Director of the NSA; Daniel Coats, in his official capacity as the Director of National Intelligence ("DNI"); and Jefferson B. Sessions, III, in his official capacity as Attorney General (collectively, the "DEFENDANTS"), and demands that DEFENDANTS answer each Request for Admission herein in writing and under oath and within thirty (30) days of the date of service of the Requests for Admission, in accordance with the Definitions and Instructions set forth below.

DEFINITIONS

Notwithstanding any definition set forth below, each word, term, or phrase used in this Request is intended to have the broadest meaning permitted under the Federal Rules of Civil

Procedure. As used in this Request, the following terms are to be interpreted in accordance with these definitions:

Answer: The term "ANSWER" means Defendants' Answer to Plaintiff's First Amended Complaint in this action, filed on October 16, 2017.

Bulk: To COPY or REVIEW INTERNET COMMUNICATIONS in "BULK" means to COPY or REVIEW INTERNET COMMUNICATIONS in large quantity without prior application of SELECTORS, or other identifiers associated with specific targets of Upstream surveillance.

Circuit: The term "CIRCUIT" has the same meaning as "circuit" in the Privacy and Civil Liberties Oversight Board's "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," dated July 2, 2014 ("PCLOB Report"), at pages 36 to 37.

Communication: The term "COMMUNICATION" means information transmitted by any means, whether orally, electronically, by document, or otherwise.

Concern or Concerning: The terms "CONCERN" and "CONCERNING" mean relating to, referring to, describing, evidencing, constituting, reflecting, memorializing, identifying, embodying, pertaining to, commenting on, discussing, analyzing, considering, containing, consisting of, indicating, supporting, refuting, or connected to.

Copy: The term "COPY" means to duplicate a piece of data (for any duration, no matter how brief).

Describe: The term "DESCRIBE" means to provide a narrative statement or description of the specific facts or matters to which an Interrogatory refers, including, but not limited to, an identification of all persons, communications, acts, transactions, events,

agreements, recommendations, and DOCUMENTS used, necessary, or desirable to support such statement or make the description complete.

Document: The term "DOCUMENT" shall have the broadest meaning ascribed to that term in Federal Rule of Civil Procedure 34 and Federal Rule of Evidence 1001. The term also includes any parent or child attachment or other documents embedded or linked in any way to a requested document. A draft or non-identical copy is a separate document within the meaning of the term "DOCUMENT."

Identify (with respect to PERSONS): When referring to a PERSON, to "IDENTIFY" means to state the PERSON's full name, present or last known address, and, when referring to a natural person, the present or last known place of employment. If the business and home telephone numbers are known to the answering party, and if the PERSON is not a party or present employee of a party, said telephone numbers shall be provided. Once a PERSON has been identified in accordance with this subparagraph, only the name of the PERSON need be listed in response to subsequent discovery requesting the identification of that PERSON.

Identify (with respect to documents): When referring to documents, to "IDENTIFY" means to state the: (i) type of document; (ii) general subject matter; (iii) date of the document; and (iv) author(s), addressee(s), and recipient(s); or, alternatively, to produce the document.

Interacted with: "INTERACTED WITH" means to have used a device to COPY or REVIEW an INTERNET COMMUNICATION or INTERNET TRANSACTION while such communication or transaction is being transmitted or while the communication or transaction is being stored, other than as necessary to transmit or store the communication.

International Communication: The term "INTERNATIONAL COMMUNICATION" means an INTERNET COMMUNICATION between at least one party in the UNITED STATES and at least one party outside the UNITED STATES.

Internet Backbone: The term "INTERNET BACKBONE" means the set of high-capacity cables, switches, and routers that facilitates both domestic and international Internet communication by parties connected to it. The INTERNET BACKBONE includes, but is not limited to, the international submarine cables that carry INTERNET COMMUNICATIONS.

Internet Communication: The term "INTERNET COMMUNICATION" means a series of related packets that are sent from a particular source to a particular destination that together constitute a message of some sort, including but not limited to an email message, an HTTP request, or an HTTP response.

Internet Packet: The term "INTERNET PACKET" means a discrete chunk of information transmitted across the Internet. All INTERNET COMMUNICATIONS are split into one or more INTERNET PACKETS. Each INTERNET PACKET contains a source and destination Internet Protocol ("IP") address and some payload.

Internet Transaction: The term "INTERNET TRANSACTION" has the same meaning as "Internet transaction" within the PCLOB Report at pages 39 and 125 and note 517.

NSA: The terms "National Security Agency" and "NSA" include any department, office, entity, officer, employee, agent, representative, attorney, consultant, or contractor thereof, as well as telecommunication providers acting at the NSA's direction.

Parties: The terms "PLAINTIFF" and "DEFENDANT," as well as a party's full or abbreviated name or a pronoun referring to a party, mean that party and its officers, directors, employees, agents, representatives, attorneys, consultants, and contractors. This definition is not

intended to impose a discovery obligation on any PERSON who is not a party to the litigation or to limit the Court's jurisdiction to enter any appropriate order.

Person: The term "PERSON" is defined as any natural person or any business, legal or governmental entity, or association.

Process: The term "PROCESS" has the same meaning as "process," "process[ed]," or "process[ing]" within the July 2014 Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended, *available at* https://www.dni.gov/files/documents/0928/2014%20NSA%20702%20Minimization%20Procedures.pdf ("2014 NSA Minimization Procedures").

Retain: The term "RETAIN" has the same meaning as "retain," "retained," or "retention" within the 2014 NSA Minimization Procedures.

Review: The term "REVIEW" means to scan, search, screen, capture, monitor, analyze, redirect, divert, or gather information about the contents of.

Selector: The term "SELECTOR" has the same meaning as "selector" within the 2014 NSA Minimization Procedures.

Target: The term "TARGET" means the subjects who are "targeted" pursuant to 50 U.S.C. § 1881a.

United States: When used as a term of geographic location, "UNITED STATES" means all areas under the territorial sovereignty of the United States.

Wholly Domestic Communication: The term "WHOLLY DOMESTIC COMMUNICATION" means an INTERNET COMMUNICATION whose origin and final destination are both located within the UNITED STATES.

You/Your: The terms "YOU" or "YOUR" include the defendant agency, and department, office, entity, officer, employee, agent, representative, attorney, consultant, or contractor thereof.

The present tense includes the past and future tenses. The singular includes the plural, and the plural includes the singular. "All" means "any and all"; "any" means "any and all." "Including" means "including but not limited to." "And" and "or" encompass both "and" and "or." Words in the masculine, feminine, or neutral form shall include each of the other genders.

INSTRUCTIONS

1. YOU are requested to answer each Request for Admission set forth below separately and completely in writing under oath. In answering these Requests for Admission, respond truthfully and in good faith on the basis of all information that is known or readily obtainable by YOU.

2. As required by Federal Rule of Civil Procedure 36(a)(4), if good faith requires that YOU deny only a portion of any matter as to which an admission is requested, or that YOU qualify any response as to any given Request for Admission, specify and admit so much of the Request as is true and deny or qualify only that portion of the Request as to which good faith requires a denial or qualification.

3. Each Request for Admission shall be answered fully unless it is objected to in good faith, in which event the reasons for YOUR objection shall be stated in detail. If an objection pertains to only a portion of a Request for Admission, or a word, phrase, or clause contained within it, YOU are required to state YOUR objection to that portion only and to respond to the remainder of the Request for Admission, using YOUR best efforts to do so.

4. If YOU assert that any information responsive to any Request for Admission is privileged or otherwise protected from discovery, YOU are requested to expressly make a claim of privilege and to describe the nature of the information not disclosed, in a manner that, without revealing information itself privileged or protected, will enable PLAINTIFF to assess the claim of privilege. For any DOCUMENT or information withheld on the grounds that it is privileged or otherwise claimed to be excludable from discovery, identify the information or DOCUMENT, describe its subject matter and date, identify all authors and all recipients (including copied and blind copied recipients), and specify the basis for the claimed privilege or other grounds of exclusion.

5. YOUR responses to these Requests should be based upon information known to YOU CONCERNING facts or events that occurred, in whole or in part, as of June 22, 2015.

6. These Requests for Admission are continuing in nature and YOUR responses to them are to be promptly supplemented or amended if, after the time of YOUR initial responses, YOU learn that any response is or has become in some material respect incomplete or incorrect, to the full extent provided for by Federal Rule of Civil Procedure 26(e).

REQUESTS FOR ADMISSION

REQUEST FOR ADMISSION NO. 1:

Admit that there are between 45 and 55 international submarine cables that carry INTERNET COMMUNICATIONS directly into or directly out of the UNITED STATES.

REQUEST FOR ADMISSION NO. 2:

Admit that the international submarine cables that carry INTERNET COMMUNICATIONS directly into or directly out of the UNITED STATES make landfall at approximately 40 to 45 different landing points within the UNITED STATES.

REQUEST FOR ADMISSION NO. 3:

Admit that the INTERNET BACKBONE includes international submarine cables that carry INTERNET COMMUNICATIONS into and out of the UNITED STATES.

REQUEST FOR ADMISSION NO. 4:

Admit that the INTERNET BACKBONE includes high-capacity terrestrial cables that carry traffic within the UNITED STATES.

REQUEST FOR ADMISSION NO. 5:

Admit that, in conducting Upstream surveillance, the NSA COPIES INTERNET COMMUNICATIONS that are in transit on the INTERNET BACKBONE, prior to RETAINING INTERNET COMMUNICATIONS that contain a SELECTOR.

REQUEST FOR ADMISSION NO. 6:

Admit that, in conducting Upstream surveillance, the NSA REVIEWS the contents of INTERNET COMMUNICATIONS that are in transit on the INTERNET BACKBONE, prior to RETAINING INTERNET COMMUNICATIONS that contain a SELECTOR.

REQUEST FOR ADMISSION NO. 7:

Admit that, in conducting Upstream surveillance, the NSA COPIES INTERNET COMMUNICATIONS in BULK that are in transit on the INTERNET BACKBONE.

REQUEST FOR ADMISSION NO. 8:

Admit that, in conducting Upstream surveillance, the NSA REVIEWS the contents of INTERNET COMMUNICATIONS in BULK that are in transit on the INTERNET BACKBONE.

REQUEST FOR ADMISSION NO. 9:

Admit that, in conducting Upstream surveillance, the NSA COPIES INTERNET COMMUNICATIONS that are neither to nor from TARGETS, prior to RETAINING INTERNET COMMUNICATIONS that contain a SELECTOR.

REQUEST FOR ADMISSION NO. 10:

Admit that, in conducting Upstream surveillance, the NSA REVIEWS the contents of INTERNET COMMUNICATIONS that are neither to nor from TARGETS, prior to RETAINING INTERNET COMMUNICATIONS that contain a SELECTOR.

REQUEST FOR ADMISSION NO. 11:

Admit that the NSA does not consider an INTERNET COMMUNICATION "collected," within the meaning of the 2014 NSA Minimization Procedures, until after it has REVIEWED the contents of the communication and has selected it for RETENTION.

REQUEST FOR ADMISSION NO. 12:

Admit that, in the course of Upstream surveillance, the NSA RETAINS WHOLLY DOMESTIC COMMUNICATIONS.

REQUEST FOR ADMISSION NO. 13:

Admit that the NSA conducts Upstream surveillance on multiple INTERNET BACKBONE CIRCUITS.

REQUEST FOR ADMISSION NO. 14:

Admit that the NSA conducts Upstream surveillance on multiple "international Internet link[s]," as that term is used by the government in its submission to the Foreign Intelligence Surveillance Court, titled "Government's Response to the Court's Briefing Order of May 9,

2011," and filed on June 1, 2011, *see* [*Redacted*], 2011 WL 10945618, at *15 (FISC Oct. 3, 2011).

REQUEST FOR ADMISSION NO. 15:

Admit that the NSA conducts Upstream surveillance at multiple INTERNET BACKBONE "chokepoints" or "choke points" (as that term is used by YOU).

REQUEST FOR ADMISSION NO. 16:

Admit that the document attached hereto as Exhibit A, titled "Why are we interested in HTTP?," is a true and correct excerpted copy of a genuine document.

REQUEST FOR ADMISSION NO. 17:

Admit that the statements within the document attached hereto as Exhibit A were made by YOUR employees on matters within the scope of their employment during the course of their employment.

REQUEST FOR ADMISSION NO. 18:

Admit that statements within the document attached hereto as Exhibit A were made by persons YOU authorized to make statements on the subjects of the statements within the document.

REQUEST FOR ADMISSION NO. 19:

Admit that the document attached hereto as Exhibit B, titled "Fingerprints and Appids," and "Fingerprints and Appids (more)," is a true and correct excerpted copy of a genuine document.

REQUEST FOR ADMISSION NO. 20:

Admit that the statements within the document attached hereto as Exhibit B were made by YOUR employees on matters within the scope of their employment during the course of their employment.

REQUEST FOR ADMISSION NO. 21:

Admit that statements within the document attached hereto as Exhibit B were made by persons YOU authorized to make statements on the subjects of the statements within the document.

REQUEST FOR ADMISSION NO. 22:

Admit that the document attached hereto as Exhibit C, "Seven Access Sites—International 'Choke Points'," is a true and correct excerpted copy of a genuine document.

REQUEST FOR ADMISSION NO. 23:

Admit that the statements within the document attached hereto as Exhibit C were made by YOUR employees on matters within the scope of their employment during the course of their employment.

REQUEST FOR ADMISSION NO. 24:

Admit that statements within the document attached hereto as Exhibit C were made by persons YOU authorized to make statements on the subjects of the statements within the document.

REQUEST FOR ADMISSION NO. 25:

Admit that the document attached hereto as Exhibit D, titled "SSO's Support to the FBI for Implementation of their Cyber FISA Orders," is a true and correct copy of a genuine document.

REQUEST FOR ADMISSION NO. 26:

Admit that the statements within the document attached hereto as Exhibit D were made by YOUR employees on matters within the scope of their employment during the course of their employment.

REQUEST FOR ADMISSION NO. 27:

Admit that statements within the document attached hereto as Exhibit D were made by persons YOU authorized to make statements on the subjects of the statements within the document.

REQUEST FOR ADMISSION NO. 28:

Admit that the document attached hereto as Exhibit E, titled "Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended" and dated July 28, 2009 (the "NSA Targeting Procedures") is a true and correct copy of a genuine document.

REQUEST FOR ADMISSION NO. 29:

Admit that the statements within the document attached hereto as Exhibit E were made by YOUR employees on matters within the scope of their employment during the course of their employment.

REQUEST FOR ADMISSION NO. 30:

Admit that statements within the document attached hereto as Exhibit E were made by persons YOU authorized to make statements on the subjects of the statements within the document.

REQUEST FOR ADMISSION NO. 31:

Admit that the document attached hereto as Exhibit F, titled "Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended," dated July 2014, and available at https://www.dni.gov/files/documents/0928/2014%20NSA%20702%20Minimization%20Procedures.pdf, is a true and correct copy of a genuine document.

REQUEST FOR ADMISSION NO. 32:

Admit that the statements within the document attached hereto as Exhibit F were made by YOUR employees on matters within the scope of their employment during the course of their employment.

REQUEST FOR ADMISSION NO. 33:

Admit that statements within the document attached hereto as Exhibit F were made by persons YOU authorized to make statements on the subjects of the statements within the document.

Dated: November 7, 2017

/s/ Ashley Gorski
Ashley Gorski
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
agorski@aclu.org

Counsel for Plaintiff

Exhibit A

Why are we interested in HTTP?

facebook

YAHOO!

twitter

myspace.com a place for friends

Because nearly everything a typical user does on the Internet uses HTTP

CNN.com

Google Earth

@mail.ru

WIKIPEDIA The Free Encyclopedia

Gmail by Google BETA

Exhibit B

Fingerprints and Appids

- Useful for identifying classes of traffic or particular targets (for SIGDEV or collection):

  mail/webmail/yahoo

  browser/cellphone/blackberry

  topic/s2B/chinese_missile

- appid – a contest, highest scoring appid wins
- fingerprint – many fingerprints per session
- microplugin – a fingerprint or appid that is relatively complex (e.g. extracts and databases metadata)

Fingerprints and Appids (more)

- Written in language called "GENESIS" (go genesis-language):

```
appid('encyclopedia/wikipedia', 2.0) =
   http_host('wikipedia' or 'wikimedia');
fingerprint('dns/malware/MalwareDomains') =
   dns_host(' erofreex.info ' or ' datayakoz.info '
   or ' erogirlx.info ' or ' pornero.info ' or ...
```

- If a fingerprint contains a `schema` definition, a search form automatically appears in the XKEYSCORE GUI
- Power users can drop in to C++ to express themselves

Exhibit C

STORMBREW At a Glance

Exhibit D

SECRET//REL TO USA, FVEY

SECURITY CLASSIFICATION

NSA STAFF PROCESSING FORM

TO	EXREG CONTROL NUMBER	KCC CONTROL NUMBER
SIGINT DIR	2012-704	S353-113-11

THRU	ACTION	EXREG SUSPENSE
	[X] APPROVAL	
SUBJECT	[ ] SIGNATURE	KCC SUSPENSE
(S//REL) SSO's Support to the FBI for Implementation of their Cyber FISA Orders	[ ] INFORMATION	ELEMENT SUSPENSE

DISTRIBUTION
V2, V3, V07

SUMMARY

RECOMMENDATION: (U//FOUO) Approve the provision of the assistance to FBI, with the proviso that the FBI remains responsible for any additional expenses incurred.

PURPOSE: (S//REL) To obtain the SIGINT Director's approval for the Office of Special Source Operations (SSO) to provide ongoing technical assistance to the Federal Bureau of Investigation (FBI) for the implementation of the various orders they have obtained, and will obtain, from the Foreign Intelligence Surveillance Court (FISC) in certain Cyber cases involving agents of foreign powers (e.g. - [redacted] soon, [redacted]). The preparation of this Staff Processing Form was a collaborative effort between SSO and the NSA Office of General Counsel (OGC).

BACKGROUND: (S//REL) On December 20, 2011, NSA received a request for technical assistance from the FBI seeking access to infrastructure established by NSA for collection of foreign intelligence from U.S. telecommunications providers. The FISC has issued a number of orders at the request of the FBI authorizing electronic surveillance directed at communications related to computer intrusions being conducted by foreign powers. The orders include some that are limited to pen register/trap and trace (PRTT) information as well as others that authorize collection of content. The first of these for which NSA assistance has been requested is directed at communications related to intrusions conducted by the [redacted] (Docket Number 11-91), regarding what FBI refers to as STYGIAN FLOW.

(S//REL) In mid-2011, prior to receipt of the request for technical assistance, SSO became aware of FBI's plans to seek these orders and has been in discussions with FBI throughout the latter half of the year, in the belief that use of NSA's collection/processing infrastructure would allow the FBI to

Continued...

COORDINATION/APPROVAL

OFFICE	NAME AND DATE	SECURE PHONE	OFFICE	NAME AND DATE	SECURE PHONE
OGC	[redacted] /email/ 30 Jan.				
F1B	[redacted] /email/ 9 Feb.		S3	[redacted] /s/ 3-20-12	
S1	[redacted] /s/		S35	[redacted]	
NTOC	[redacted] /s/		SV	[redacted] /s/ 31 Jan.	
T	[redacted] /s/ 6 Feb		POC	[redacted]	[redacted]

ORIGINATOR	ORG.	PHONE (Secure)	DATE PREPARED
[redacted] Digitally signed by [redacted] DN: c=US, [redacted] ou=NSA, ou=D002, [redacted] Date: 2011.12.21 07:42:01 -05'00'	S353	[redacted]	20111221

FORM A6796DE REV NOV 2008(Supersedes A6796 FEB 05 which is obsolete)
NSN: 7540-FM-001-5465
Derived From: NSA/CSS Manual 1-52
Dated: 8 January 2007
Declassify On: 20320108

SECURITY CLASSIFICATION
SECRET//REL TO USA, FVEY

maximize the value of the collection without incurring the expenses associated with duplication of that infrastructure. Although FBI conducts numerous electronic surveillances without NSA's assistance, the vast majority of them are directed against targets located inside the United States, and U.S. providers served with FISC orders are ordinarily able to identify and deliver to the FBI most, if not all, of the targets' communications that they carry. That is because such electronic surveillance is typically effected at a point or points in the provider's infrastructure in physical proximity to the target's location. In the case of computer intrusions being conducted by foreign powers, the providers may be carrying a target's communications, but it is much more difficult to identify and locate them, because the communications in question will enter and leave the United States via any convenient path, and their path may be obscured to avoid detection. In other words, in these cases, because the target's location is outside the United Statues and not well-characterized, effecting the surveillance via FBI's traditional means is not effective.

(S//REL) However, in support of FAA and in anticipation of the need to conduct similar collection activities for computer network defense purposes, over the last decade, NSA has expended a significant amount of resources to create collection/processing capabilities at many of the chokepoints operated by U.S. providers through which international communications enter and leave the United States. Collection at such chokepoints is much better suited to electronic surveillance directed at targets located outside the United States than FBI's traditional means of collection. In theory, FBI could rely on the orders it has obtained to direct U.S. providers to conduct surveillance at these chokepoints without relying on NSA capabilities, but it would take a considerable amount of time to do so, and FBI would have to reimburse the providers to recreate (i.e., duplicate) what NSA has already put in place. The cost alone would be prohibitive, and the time lost in doing so would necessarily result in a loss of foreign intelligence.

(S//REL) The assistance being sought by the FBI is limited in nature. The U.S. providers served with Secondary Orders in this matter will assume full responsibility for the provisioning of PR/TT and content collection to the FBI. Since all of the authorized "facilities" (typically known as "targeted selectors" in NSA parlance) to date are Internet Protocol (IP) addresses used by the targets, there is no question as to the providers' abilities to employ devices under their control (e.g., routers) to provision fully-compliant, authorized intercept.

(S//REL) Neither the providers nor the FBI will require NSA's Government off the Shelf (GOTS) Digital Network Intelligence (DNI) collection and processing solutions (e.g., TURMOIL, XKEYSCORE). Instead, metadata and full content derived from the authorized intercept will be produced using Commercial off the Shelf (COTS) processing solutions. If these COTS processing solutions involve components developed at NSA's expense and used, primarily, for NSA's Cyber survey purposes, the SSO will make careful and informed decisions prior to authorizing use of these components.

Page 3 of 4: CATS 2012-704 (S//REL TO USA, FVEY) SSO's Support to the FBI for Implementation of their Cyber FISA Orders

(S//REL) Prior to authorizing use of the extensive secure Wide Area Networks established at the two primary providers (cover terms, LITHIUM and ARTIFICE, respectively) as the end-to-end data delivery infrastructure to connect intercept and processing locations with the FBI's designated Cyber data repository at the Engineering Research Facility, Quantico, VA, SSO will make careful and informed decisions to ensure this capability is undertaken on a 100% non-interference basis with NSA's current and future data backhaul needs on these same networks.

(S//REL) All data (metadata and/or content) collected under the auspices of these FISC orders will be forwarded securely and directly to the designated FBI repository. The FISC orders do contain a provision, as follows: "NCIJTF personnel participating in this joint investigation may have access to raw data prior to minimization." However, access to raw data by NTOC members of the NCIJTF will be facilitated under the purview of the FBI and not through any actions that SSO might take as the collected data passes through NSA's secure Wide Area Networks. Should the FBI's cyber orders from the FISC be modified in the future to authorize raw data retention by NSA, SSO will coordinate with all cognizant NSA offices (e.g., Data Governance, OGC, SV) to ensure the proper data delivery mechanism is put in place.

(S//REL) Should the FBI require a sustained and high-level of dedicated analytical resources (i.e., cleared, technical manpower) at the providers in order to optimize the collection effectiveness of their PR/TT and content orders, they will contract for those services directly with the providers. If, on the other hand, the FBI's requirement for provider analytical support is more ad hoc and aperiodic in nature during the period of time these orders remain in effect, SSO will make careful and informed decisions prior to authorizing labor charges against the relevant SSO contracts with the providers for these services on behalf of the FBI. Any charges that cannot be justified as necessary for NSA purposes will not be made unless/until FBI agrees to reimburse NSA.

DISCUSSION: (S//REL) If SID decides to approve the requested assistance, SSO will assist the FBI in effecting any cyber orders submitted to it after the NSA/OGC has verified that each of them contains language permitting NSA's involvement. As stated in Attachment 1, NSA will have the opportunity to review and respond to any proposed use of FISA-derived information from these collections prior to the Attorney General authorizing the use of such information in any criminal proceedings.

(S//REL) The assistance SSO is being asked to provide to the FBI will not preclude NSA's SIGINT targeting of these same fully-qualified, overseas IP addresses under the auspices of the FISA

Continued...

(S//REL) The assistance SSO is being asked to provide to the FBI will not preclude NSA's SIGINT targeting of these same fully-qualified, overseas IP addresses under the auspices of the FISA Amendments Act (FAA) of 2008. To the contrary, the relatively recent discovery of these FBI Cyber FISA orders and the countless pages of SIGINT-derived evidence that was cited in the respective Applications to the FISC have already formed the basis for a dialog between NSA's OGC and the Department of Justice's National Security Division.

(C) DIRECTOR, SIGNALS INTELLIGENCE DECISION:

CONCUR: Teresa H. Shea DATE: 3-827-12

NON-CONCUR:_____ DATE:_____

Exhibit E

EXHIBIT A

PROCEDURES USED BY THE NATIONAL SECURITY AGENCY FOR TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES TO ACQUIRE FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED

(S) These procedures address: (I) the manner in which the National Security Agency/Central Security Service (NSA) will determine that a person targeted under section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended ("the Act"), is a non-United States person reasonably believed to be located outside the United States ("foreignness determination"); (II) the post-targeting analysis done by NSA to ensure that the targeting of such person does not intentionally target a person known at the time of acquisition to be located in the United States and does not result in the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States; (III) the documentation of NSA's foreignness determination; (IV) compliance and oversight; and (V) departures from these procedures.

I. (U) DETERMINATION OF WHETHER THE ACQUISITION TARGETS NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES

(S) NSA determines whether a person is a non-United States person reasonably believed to be outside the United States in light of the totality of the circumstances based on the information available with respect to that person, including information concerning the communications facility or facilities used by that person.

(S) NSA analysts examine the following three categories of information, as appropriate under the circumstances, to make the above determination: (1) they examine the lead information they have received regarding the potential target or the facility that has generated interest in conducting surveillance to determine what that lead information discloses about the person's location; (2) they conduct research in NSA databases, available reports and collateral information (i.e., information to which NSA has access but did not originate, such as reports from other agencies and publicly available information) to determine whether NSA knows the location of the person, or knows information that would provide evidence concerning that location; and (3) they conduct technical analyses of the facility or facilities to determine or verify information about the person's location. NSA may use information from any one or a combination of these categories of information in evaluating the totality of the circumstances to determine that the potential target is located outside the United States.

(TS//SI) In addition, in those cases where NSA seeks to acquire communications about the target that are not to or from the target, NSA will either employ an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

overseas, or it will target Internet links that terminate in a foreign country. In either event, NSA will direct surveillance at a party to the communication reasonably believed to be outside the United States.

(S) Lead Information

(S) When NSA proposes to direct surveillance at a target, it does so because NSA has already learned something about the target or the facility or facilities the target uses to communicate. Accordingly, NSA will examine the lead information to determine what it reveals about the physical location of the target, including the location of the facility or facilities being used by the potential target.

(S) The following are examples of the types of lead information that NSA may examine:

a) Has the target stated that he is located outside the United States? For example, has NSA or another intelligence agency collected a statement or statements made by the target indicating that he is located outside the United States?

b) Has a human intelligence source or other source of lead information indicated that the target is located outside the United States?

c) Does the lead information provided by an intelligence or law enforcement agency of the United States government or an intelligence or law enforcement service of a foreign government indicate that the target is located outside the United States?

d) Was the lead information about the target found on a hard drive or other medium that was seized in a foreign country?

e) With whom has the target had direct contact, and what do we know about the location of such persons? For example, if lead information indicates the target is in direct contact with several members of a foreign-based terrorist organization or foreign-based political organization who themselves are located overseas, that may suggest, depending on the totality of the circumstances, that the target is also located overseas.

(S) Information NSA Has About the Target's Location and/or Facility or Facilities Used by the Target

(S) NSA may also review information in its databases, including repositories of information collected by NSA and by other intelligence agencies, as well as publicly available information, to determine if the person's location, or information providing evidence about the person's location, is already known. The NSA databases that would be used for this purpose contain information culled from signals intelligence, human intelligence, law enforcement information, and other sources. For example, NSA databases may include a report produced by the Central Intelligence Agency (CIA) with the fact that a known terrorist is using a telephone with a particular number, or detailed information on worldwide telephony numbering plans for wire and wireless telephone systems.

(S) NSA Technical Analysis of the Facility

(S) NSA may also apply technical analysis concerning the facility from which it intends to acquire foreign intelligence information to assist it in making determinations concerning the location of the person at whom NSA intends to direct surveillance. For example, NSA may examine the following types of information:

(S) For telephone numbers:

a) Identify the country code of the telephone number, and determine what it indicates about the person's location.

b) Review commercially available and NSA telephone numbering databases for indications of the type of telephone being used (e.g. landline, wireless mobile, satellite, etc.), information that may provide an understanding of the location of the target.

(S) For electronic communications accounts/addresses/identifiers:

Review NSA content repositories and Internet communications data repositories (which contain, among other things, Internet communications metadata) for previous Internet activity. This information may contain network layer (e.g., Internet Protocol addresses) or machine identifier (e.g., Media Access Control addresses) information, which NSA compares to information contained in NSA's communication network databases and commercially available Internet Protocol address registration information in order to determine the location of the target.

(S) Assessment of the Non-United States Person Status of the Target

(S) In many cases, the information that NSA examines in order to determine whether a target is reasonably believed to be located outside the United States may also bear upon the non-United States person status of that target. For example, lead information provided by an intelligence or law enforcement service of a foreign government may indicate not only that the target is located in a foreign country, but that the target is a citizen of that or another foreign country. Similarly, information contained in NSA databases, including repositories of information collected by NSA and by other intelligence agencies, may indicate that the target is a non-United States person.

(S) Furthermore, in order to prevent the inadvertent targeting of a United States person, NSA maintains records of telephone numbers and electronic communications accounts/addresses/identifiers that NSA has reason to believe are being used by United States persons. Prior to targeting, a particular telephone number or electronic communications account/address/identifier will be compared against those records in order to ascertain whether NSA has reason to believe that telephone number or electronic communications account/address/identifier is being used by a United States person.

(S) In the absence of specific information regarding whether a target is a United States person, a person reasonably believed to be located outside the United States or whose location is not known will be presumed to be a non-United States person unless such person can be positively identified as a United States person, or the nature or circumstances of the person's communications give rise to a reasonable belief that such person is a United States person.

(S) Assessment of the Foreign Intelligence Purpose of the Targeting

(S) In assessing whether the target possesses and/or is likely to communicate foreign intelligence information concerning a foreign power or foreign territory, NSA considers, among other things, the following factors:

a. With respect to telephone communications:

- Information indicates that the telephone number has been used to communicate directly with another telephone number reasonably believed by the U.S. Intelligence Community to be used by an individual associated with a foreign power or foreign territory;
- Information indicates that a user of the telephone number has communicated directly with an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;
- Information indicates that the telephone number is listed in the telephone directory of a telephone used by an individual associated with a foreign power or foreign territory;
- Information indicates that the telephone number has been transmitted during a telephone call or other communication with an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;
- Publicly available sources of information (e.g., telephone listings) match the telephone number to an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;
- Information contained in various NSA-maintained knowledge databases containing foreign intelligence information acquired by any lawful means, such as electronic surveillance, physical search, or the use of a pen register and trap or trace device, or other information, reveals that the telephone number has been previously used by an individual associated with a foreign power or foreign territory;[1] or

[1] (TS//SI//NF) The NSA knowledge databases that would be used to satisfy this factor contain fused intelligence information concerning international terrorism culled from signals intelligence, human intelligence, law enforcement information, and other sources. The information compiled in these databases is information that assists the signals intelligence system in effecting collection on intelligence targets. For example, a report produced by the CIA may include the fact that a known terrorist is using a telephone with a particular number. NSA would include that information in its knowledge databases.

- Information made available to NSA analysts as a result of processing telephony metadata records acquired by any lawful means, such as electronic surveillance, physical search, or the use of a pen register or trap and trace device, or other information, reveals that the telephone number is used by an individual associated with a foreign power or foreign territory.

b. With respect to Internet communications:

- Information indicates that the electronic communications account/address/identifier has been used to communicate directly with an electronic communications account/address/identifier reasonably believed by the U.S. Intelligence Community to be used by an individual associated with a foreign power or foreign territory;

- Information indicates that a user of the electronic communications account/address/identifier has communicated directly with an individual reasonably believed to be associated with a foreign power or foreign territory;

- Information indicates that the electronic communications account/address/identifier is included in the "buddy list" or address book of an electronic communications account/address/identifier reasonably believed by the U.S. Intelligence Community to be used by an individual associated with a foreign power or foreign territory;

- Information indicates that the electronic communications account/address/identifier has been transmitted during a telephone call or other communication with an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;

- Public Internet postings match the electronic communications account/address/identifier to an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;

- Information contained in various NSA-maintained knowledge databases of foreign intelligence information acquired by any lawful means, such as electronic surveillance, physical search, the use of a pen register or trap and trace device, or other information, reveals that electronic communications account/address/identifier has been previously used by an individual associated with a foreign power or foreign territory;

- Information made available to NSA analysts as a result of processing metadata records acquired by any lawful means, such as electronic surveillance, physical search, or the use of a pen register or trap and trace device, or other information, reveals that the electronic communications account/address/identifier is used by an individual associated with a foreign power or foreign territory; or

- Information indicates that Internet Protocol ranges and/or specific electronic identifiers or signatures (e.g., specific types of cryptology or steganography) are used almost exclusively by individuals associated with a foreign power or foreign territory,

or are extensively used by individuals associated with a foreign power or foreign territory.

II. (S) POST-TARGETING ANALYSIS BY NSA

(S//SI) After a person has been targeted for acquisition by NSA, NSA will conduct post-targeting analysis. Such analysis is designed to detect those occasions when a person who when targeted was reasonably believed to be located outside the United States has since entered the United States, and will enable NSA to take steps to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States, or the intentional targeting of a person who is inside the United States. Such analysis may include:

For telephone numbers:

- Routinely comparing telephone numbers tasked pursuant to these procedures against information that has been incidentally collected from the Global System for Mobiles (GSM) Home Location Registers (HLR). These registers receive updates whenever a GSM phone moves into a new service area. Analysis of this HLR information provides a primary indicator of a foreign user of a mobile telephone entering the United States.

- NSA analysts may analyze content for indications that a foreign target has entered or intends to enter the United States. Such content analysis will be conducted according to analytic and intelligence requirements and priorities.

For electronic communications accounts/addresses/identifiers:

- Routinely checking all electronic communications accounts/addresses/identifiers tasked pursuant to these procedures against available databases that contain Internet communications data (including metadata) to determine if an electronic communications account/address/identifier was accessed from overseas. Such databases contain communications contact information and summaries of communications activity from NSA signals intelligence collection. The foreign access determination is made based on comparing the Internet Protocol address associated with the account activity to other information NSA possesses about geographical area(s) serviced by particular Internet Protocol addresses. If the IP address associated with the target activity is identified as a U.S.-based network gateway (e.g., a Hotmail server) or a private Internet Protocol address, then NSA analysts will be required to perform additional research to determine if the access was in a foreign country using additional criteria such as machine identifier or case notation (NSA circuit identifier) of a communications link known to be foreign. Such databases normally maintain information about such activity for a 12-month period. This data will be used in an attempt to rule out false positives from U.S.-based network gateways. If the account access is determined to be from a U.S.-based machine, further analytic checks will be performed using content collection to determine if the target has moved into the United States.

- Routinely comparing electronic communications accounts/addresses/identifiers tasked pursuant to these procedures against a list of electronic communications accounts/ addresses/identifiers already identified by NSA as being accessed from inside the United States. This will help ensure that no target has been recognized to be located in the United States.

- NSA analysts may analyze content for indications that a target has entered or intends to enter the United States. Such content analysis will be conducted according to analytic and intelligence requirements and priorities.

(S) If NSA determines that a target has entered the United States, it will follow the procedures set forth in section IV of this document, including the termination of the acquisition from the target without delay. In cases where NSA cannot resolve an apparent conflict between information indicating that the target has entered the United States and information indicating that the target remains located outside the United States, NSA will presume that the target has entered the United States and will terminate the acquisition from that target. If at a later time NSA determines that the target is in fact located outside the United States, NSA may re-initiate the acquisition in accordance with these procedures.

(S) If NSA determines that a target who at the time of targeting was believed to be a non-United States person was in fact a United States person, it will follow the procedures set forth in section IV of this document, including the termination of the acquisition from the target without delay.

III. (U) DOCUMENTATION

(S) Analysts who request tasking will document in the tasking database a citation or citations to the information that led them to reasonably believe that a targeted person is located outside the United States. Before tasking is approved, the database entry for that tasking will be reviewed in order to verify that the database entry contains the necessary citations.

(S) A citation is a reference that identifies the source of the information, such as a report number or communications intercept identifier, which NSA will maintain. The citation will enable those responsible for conducting oversight to locate and review the information that led NSA analysts to conclude that a target is reasonably believed to be located outside the United States.

(S) Analysts also will identify the foreign power or foreign territory about which they expect to obtain foreign intelligence information pursuant to the proposed targeting.

IV. (U) OVERSIGHT AND COMPLIANCE

(S) NSA's Signals Intelligence Directorate (SID) Oversight and Compliance, with NSA's Office of General Counsel (OGC), will develop and deliver training regarding the applicable procedures to ensure intelligence personnel responsible for approving the targeting of persons under these procedures, as well as analysts with access to the acquired foreign intelligence information understand their responsibilities and the procedures that apply to this acquisition. SID Oversight and Compliance has established processes for ensuring that raw traffic is labeled and stored only in authorized repositories, and is accessible only to those who have had the proper training. SID

Oversight and Compliance will conduct ongoing oversight activities and will make any necessary reports, including those relating to incidents of noncompliance, to the NSA Inspector General and OGC, in accordance with its NSA charter. SID Oversight and Compliance will also ensure that necessary corrective actions are taken to address any identified deficiencies. To that end, SID Oversight and Compliance will conduct periodic spot checks of targeting decisions and intelligence disseminations to ensure compliance with established procedures, and conduct periodic spot checks of queries in data repositories.

(S) The Department of Justice (DOJ) and the Office of the Director of National Intelligence (ODNI) will conduct oversight of NSA's exercise of the authority under section 702 of the Act, which will include periodic reviews by DOJ and ODNI personnel to evaluate the implementation of the procedures. Such reviews will occur at least once every sixty days.

(S) NSA will report to DOJ, to the ODNI Office of General Counsel, and to the ODNI Civil Liberties Protection Officer any incidents of noncompliance with these procedures by NSA personnel that result in the intentional targeting of a person reasonably believed to be located in the United States, the intentional targeting of a United States person, or the intentional acquisition of any communication in which the sender and all intended recipients are known at the time of acquisition to be located within the United States. NSA will provide such reports within five business days of learning of the incident. Any information acquired by intentionally targeting a United States person or a person not reasonably believed to be outside the United States at the time of such targeting will be purged from NSA databases.

(S) NSA will report to DOJ through the Deputy Assistant Attorney General in the National Security Division with responsibility for intelligence operations and oversight, to the ODNI Office of General Counsel, and to the ODNI Civil Liberties Protection Officer, any incidents of noncompliance (including overcollection) by any electronic communication service provider to whom the Attorney General and Director of National Intelligence issued a directive under section 702. Such report will be made within five business days after determining that the electronic communication service provider has not complied or does not intend to comply with a directive.

(S) In the event that NSA concludes that a person is reasonably believed to be located outside the United States and after targeting this person learns that the person is inside the United States, or if NSA concludes that a person who at the time of targeting was believed to be a non-United States person was in fact a United States person, it will take the following steps:

1) Terminate the acquisition without delay and determine whether to seek a Court order under another section of the Act. If NSA inadvertently acquires a communication sent to or from the target while the target is or was located inside the United States, including any communication where the sender and all intended recipients are reasonably believed to be located inside the United States at the time of acquisition, such communication will be treated in accordance with the applicable minimization procedures.

2) Report the incident to DOJ through the Deputy Assistant Attorney General in the National Security Division with responsibility for intelligence operations and oversight, to the ODNI Office of General Counsel, and to the ODNI Civil Liberties Protection Officer within five business days.

V. (U) DEPARTURE FROM PROCEDURES

(S) If, in order to protect against an immediate threat to the national security, NSA determines that it must take action, on a temporary basis, in apparent departure from these procedures and that it is not feasible to obtain a timely modification of these procedures from the Attorney General and Director of National Intelligence, NSA may take such action and will report that activity promptly to DOJ through the Deputy Assistant Attorney General in the National Security Division with responsibility for intelligence operations and oversight, to the ODNI Office of General Counsel, and to the ODNI Civil Liberties Protection Officer. Under such circumstances, the Government will continue to adhere to all of the statutory limitations set forth in subsection 702(b) of the Act.

7-28-09
Date

Eric H. Holder, Jr.
Attorney General of the United States

Exhibit F

EXHIBIT B

MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED

(U) Section 1 - Applicability and Scope

(U) These National Security Agency (NSA) minimization procedures apply to the acquisition, retention, use, and dissemination of information, including non-publicly available information concerning unconsenting United States persons, that is acquired by targeting non-United States persons reasonably believed to be located outside the United States in accordance with section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended (FISA or "the Act").

(U) If NSA determines that it must take action in apparent departure from these minimization procedures to protect against an immediate threat to human life (e.g., force protection or hostage situations) and that it is not feasible to obtain a timely modification of these procedures, NSA may take such action immediately. NSA will report the action taken to the Office of the Director of National Intelligence and to the National Security Division of the Department of Justice, which will promptly notify the Foreign Intelligence Surveillance Court of such activity.

~~(S//NF)~~ Nothing in these procedures shall restrict NSA's performance of lawful oversight functions of its personnel or systems, or lawful oversight functions of the Department of Justice's National Security Division, Office of the Director of National Intelligence, or the applicable Offices of the Inspectors General. Additionally, nothing in these procedures shall restrict NSA's ability to conduct vulnerability or network assessments using information acquired pursuant to section 702 of the Act in order to ensure that NSA systems are not or have not been compromised. Notwithstanding any other section in these procedures, information used by NSA to conduct vulnerability or network assessments may be retained for one year solely for that limited purpose. Any information retained for this purpose may be disseminated only in accordance with the applicable provisions of these procedures.

(U) For the purposes of these procedures, the terms "National Security Agency" and "NSA personnel" refer to any employees of the National Security Agency/Central Security Service ("NSA/CSS" or "NSA") and any other personnel engaged in Signals Intelligence (SIGINT) operations authorized pursuant to section 702 of the Act if such operations are executed under the direction, authority, or control of the Director, NSA/Chief, CSS (DIRNSA).

(U) Section 2 - Definitions

(U) In addition to the definitions in sections 101 and 701 of the Act, the following definitions will apply to these procedures:

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: ~~20320108~~

(a) (U) Acquisition means the collection by NSA or the Federal Bureau of Investigation (FBI) through electronic means of a non-public communication to which it is not an intended party.

(b) (U) Communications concerning a United States person include all communications in which a United States person is discussed or mentioned, except where such communications reveal only publicly available information about the person.

(c) (U) Communications of a United States person include all communications to which a United States person is a party.

(d) (U) Consent is the agreement by a person or organization to permit the NSA to take particular actions that affect the person or organization. To be effective, consent must be given by the affected person or organization with sufficient knowledge to understand the action that may be taken and the possible consequences of that action. Consent by an organization will be deemed valid if given on behalf of the organization by an official or governing body determined by the General Counsel, NSA, to have actual or apparent authority to make such an agreement.

(e) (U) Foreign communication means a communication that has at least one communicant outside of the United States. All other communications, including communications in which the sender and all intended recipients are reasonably believed to be located in the United States at the time of acquisition, are domestic communications.

(f) (U) Identification of a United States person means (1) the name, unique title, or address of a United States person; or (2) other personal identifiers of a United States person when appearing in the context of activities conducted by that person or activities conducted by others that are related to that person. A reference to a product by brand name, or manufacturer's name or the use of a name in a descriptive sense, e.g., "Monroe Doctrine," is not an identification of a United States person.

(g) ~~(TS//SI//NF)~~ Internet transaction, for purposes of these procedures, means an Internet communication that is acquired through NSA's upstream collection techniques. An Internet transaction may contain information or data representing either a discrete communication [redacted] or multiple discrete communications [redacted]

(h) (U) Processed or processing means any step necessary to convert a communication into an intelligible form intended for human inspection.

(i) (U) Publicly available information means information that a member of the public could obtain on request, by research in public sources, or by casual observation.

(j) (U) Technical data base means information retained for cryptanalytic, traffic analytic, or signal exploitation purposes.

(k) (U) United States person means a United States person as defined in the Act. The following guidelines apply in determining whether a person whose status is unknown is a United States person:

(1) (U) A person known to be currently in the United States will be treated as a United States person unless positively identified as an alien who has not been admitted for permanent residence, or unless the nature or circumstances of the person's communications give rise to a reasonable belief that such person is not a United States person.

(2) (U) A person known to be currently outside the United States, or whose location is unknown, will not be treated as a United States person unless such person can be positively identified as such, or the nature or circumstances of the person's communications give rise to a reasonable belief that such person is a United States person.

(3) (U) A person who at any time has been known to have been an alien admitted for lawful permanent residence is treated as a United States person. Any determination that a person who at one time was a United States person (including an alien admitted for lawful permanent residence) is no longer a United States person must be made in consultation with the NSA Office of General Counsel.

(4) (U) An unincorporated association whose headquarters or primary office is located outside the United States is presumed not to be a United States person unless there is information indicating that a substantial number of its members are citizens of the United States or aliens lawfully admitted for permanent residence.

(U) Section 3 - Acquisition and Handling - General

(a) (U) Acquisition

(U) The acquisition of information by targeting non-United States persons reasonably believed to be located outside the United States pursuant to section 702 of the Act will be effected in accordance with an authorization made by the Attorney General and Director of National Intelligence pursuant to subsection 702(a) of the Act and will be conducted in a manner designed, to the greatest extent reasonably feasible, to minimize the acquisition of information not relevant to the authorized purpose of the acquisition.

(b) (U) Monitoring, Recording, and Handling

(1) (U) Personnel will exercise reasonable judgment in determining whether information acquired must be minimized and will destroy inadvertently acquired communications of or concerning a United States person at the earliest practicable point at which such communication can be identified either: as clearly not relevant to the authorized purpose of the acquisition (e.g., the communication does not contain foreign intelligence information); or, as not containing evidence of a crime which may be

disseminated under these procedures. Except as provided for in subsection 3(c) below, such inadvertently acquired communications of or concerning a United States person may be retained no longer than five years from the expiration date of the certification authorizing the collection in any event.

(2) (U) Communications of or concerning United States persons that may be related to the authorized purpose of the acquisition may be forwarded to analytic personnel responsible for producing intelligence information from the collected data. Such communications or information may be retained and disseminated only in accordance with Sections 3, 4, 5, 6, and 8 of these procedures.

(3) (U//~~FOUO~~) As a communication is reviewed, NSA analyst(s) will determine whether it is a domestic or foreign communication to, from, or about a target and is reasonably believed to contain foreign intelligence information or evidence of a crime for purposes of assessing how the communication should be handled in accordance with these procedures.

(4) (U) Handling of Internet Transactions Acquired Through NSA Upstream Collection Techniques

a. (~~TS//SI//NF~~) NSA will take reasonable steps post-acquisition to identify and segregate through technical means Internet transactions that cannot be reasonably identified as containing single, discrete communications where: the active user of the transaction (i.e., the electronic communications account/address/identifier used to send or receive the Internet transaction to or from a service provider) is reasonably believed to be located in the United States; or the location of the active user is unknown.

1. (~~TS//SI//NF~~) Notwithstanding subsection 3(b)(4)a. above, NSA may process Internet transactions acquired through NSA upstream collection techniques in order to render such transactions intelligible to analysts.

2. (~~TS//SI//NF~~) Internet transactions that are identified and segregated pursuant to subsection 3(b)(4)a. will be retained in an access-controlled repository that is accessible only to NSA analysts who have been trained to review such transactions for the purpose of identifying those that contain discrete communications as to which the sender and all intended recipients are reasonably believed to be located in the United States.

(a) (~~TS//SI//NF~~) Any information contained in a segregated Internet transaction (including metadata) may not be moved or copied from the segregated repository or otherwise used for foreign intelligence purposes unless it has been determined that the transaction does not contain any discrete communication as to which the sender and all intended recipients are reasonably believed to be located in the United States. Any Internet transaction that is identified and segregated pursuant to subsection

3(b)(4)a. and is subsequently determined to contain a discrete communication as to which the sender and all intended recipients are reasonably believed to be located in the United States will be handled in accordance with Section 5 below.

(b) (U//~~FOUO~~) Any information moved or copied from the segregated repository into repositories more generally accessible to NSA analysts will be handled in accordance with subsection 3(b)(4)b. below and the other applicable provisions of these procedures.

(c) (U//~~FOUO~~) Any information moved or copied from the segregated repository into repositories more generally accessible to NSA analysts will be marked, tagged, or otherwise identified as having been previously segregated pursuant to subsection 3(b)(4)a.

3. ~~(TS//SI//NF)~~ Internet transactions that are not identified and segregated pursuant to subsection 3(b)(4)a. will be handled in accordance with subsection 3(b)(4)b. below and the other applicable provisions of these procedures.

b. (U) NSA analysts seeking to use (for example, in a FISA application, intelligence report, or section 702 targeting) a discrete communication within an Internet transaction that contains multiple discrete communications will assess whether the discrete communication: 1) is a communication as to which the sender and all intended recipients are located in the United States; and 2) is to, from, or about a tasked selector, or otherwise contains foreign intelligence information.

1. ~~(TS//SI//NF)~~ If an NSA analyst seeks to use a discrete communication within an Internet transaction that contains multiple discrete communications, the analyst will first perform checks to determine the locations of the sender and intended recipients of that discrete communication to the extent reasonably necessary to determine whether the sender and all intended recipients of that communication are located in the United States. If an analyst determines that the sender and all intended recipients of a discrete communication within an Internet transaction are located in the United States, the Internet transaction will be handled in accordance with Section 5 below.

2. (U) If an NSA analyst seeks to use a discrete communication within an Internet transaction that contains multiple discrete communications, the analyst will assess whether the discrete communication is to, from, or about a tasked selector, or otherwise contains foreign intelligence information.

(a) (U) If the discrete communication is to, from, or about a tasked selector, any U.S. person information in that communication will be handled in accordance with the applicable provisions of these procedures.

(b) (U) If the discrete communication is not to, from, or about a tasked selector but otherwise contains foreign intelligence information, and the discrete communication is not to or from an identifiable U.S. person or a person reasonably believed to be located in the United States, that communication (including any U.S. person information therein) will be handled in accordance with the applicable provisions of these procedures.

(c) (U) If the discrete communication is not to, from, or about a tasked selector but is to or from an identifiable U.S. person, or a person reasonably believed to be located in the United States, the NSA analyst will document that determination in the relevant analytic repository or tool if technically possible or reasonably feasible. Such discrete communication cannot be used for any purpose other than to protect against an immediate threat to human life (e.g., force protection or hostage situations). NSA will report any such use to the Office of the Director of National Intelligence and to the National Security Division of the Department of Justice, which will promptly notify the Foreign Intelligence Surveillance Court of such use.

3. ~~(TS//SI//NF)~~ An NSA analyst seeking to use a discrete communication within an Internet transaction that contains multiple discrete communications in a FISA application, intelligence report, or section 702 targeting must appropriately document the verifications required by subsections 3(b)(4)b.1. and 2. above.

4. ~~(TS//SI//NF)~~ Notwithstanding subsection 3(b)(4)b. above, NSA may use metadata extracted from Internet transactions acquired on or after October 31, 2011, that are not identified and segregated pursuant to subsection 3(b)(4)a. without first assessing whether the metadata was extracted from: a) a discrete communication as to which the sender and all intended recipients are located in the United States; or b) a discrete communication to, from, or about a tasked selector. Any metadata extracted from Internet transactions that are not identified and segregated pursuant to subsection 3(b)(4)a. above will be handled in accordance with the applicable provisions of these procedures. Any metadata extracted from an Internet transaction subsequently determined to contain a discrete communication as to which the sender and all intended recipients are reasonably believed to be located inside the United States shall be destroyed upon recognition.

(5) (U) Magnetic tapes or other storage media containing communications acquired pursuant to section 702 may be scanned by computer to identify and select communications for analysis. Computer selection terms used for scanning, such as telephone numbers, key words or phrases, or other discriminators, will be limited to those selection terms reasonably likely to return foreign intelligence information. Identifiers of an identifiable U.S. person may not be used as terms to identify and select for analysis any Internet communication acquired through NSA's upstream

collection techniques. Any use of United States person identifiers as terms to identify and select communications must first be approved in accordance with NSA procedures. NSA will maintain records of all United States person identifiers approved for use as selection terms. The Department of Justice's National Security Division and the Office of the Director of National Intelligence will conduct oversight of NSA's activities with respect to United States persons that are conducted pursuant to this paragraph.

(6) (U) Further handling, retention, and dissemination of foreign communications will be made in accordance with Sections 4, 6, 7, and 8 as applicable, below. Further handling, storage, and dissemination of inadvertently acquired domestic communications will be made in accordance with Sections 4, 5, and 8 below.

(c) (U) Destruction of Raw Data

(1) ~~(S//SI~~ [redacted] Telephony communications and Internet communications acquired by or with the assistance of the FBI from Internet Service Providers that do not meet the retention standards set forth in these procedures and that are known to contain communications of or concerning United States persons will be destroyed upon recognition. Telephony communications and Internet communications acquired by or with the assistance of the FBI from Internet Service Providers may not be retained longer than five years from the expiration date of the certification authorizing the collection unless NSA specifically determines that each such communication meets the retention standards in these procedures.

(2) ~~(TS//SI//NF)~~ Internet transactions acquired through NSA's upstream collection techniques that do not contain any information that meets the retention standards set forth in these procedures and that are known to contain communications of or concerning United States persons will be destroyed upon recognition. An Internet transaction may not be retained longer than two years from the expiration date of the certification authorizing the collection unless NSA specifically determines that at least one discrete communication within the Internet transaction meets the retention standards in these procedures and that each discrete communication within the transaction either: (a) is to, from, or about a tasked selector; or (b) is not to, from, or about a tasked selector and is also not to or from an identifiable United States person or person reasonably believed to be in the United States. The Internet transactions that may be retained include those that were acquired because of limitations on NSA's ability to filter communications. Any Internet communications acquired through NSA's upstream collection techniques that are retained in accordance with this subsection may be reviewed and handled only in accordance with the standards set forth above in subsection 3(b)(4) of these procedures.

(3) ~~(TS//SI//NF)~~ Any Internet transactions acquired through NSA's upstream collection techniques prior to October 31, 2011, will be destroyed upon recognition.

(4) ~~(S//NF)~~ NSA may temporarily retain specific section 702-acquired information that would otherwise have to be destroyed, pursuant to section 3(a)-(c) above, if the Department of Justice advises NSA in writing that such information is subject to a preservation obligation in pending or anticipated administrative, civil, or criminal litigation. The specific information to be retained (including, but not limited to, the target(s) or selector(s) whose unminimized information must be preserved and the relevant time period at issue in the litigation), and the particular litigation for which the information will be retained, shall be identified in writing by the Department of Justice. Personnel not working on the particular litigation matter shall not access the unminimized section 702-acquired information preserved pursuant to a written preservation notice from the Department of Justice that would otherwise have been destroyed pursuant to these procedures. Other personnel shall only access the information being retained for litigation-related reasons on a case-by-case basis after consultation with the Department of Justice. The Department of Justice shall notify NSA in writing once the section 702-acquired information is no longer required to be preserved for such litigation matters, and then NSA shall promptly destroy the section 702-acquired information as otherwise required by these procedures. Circumstances could arise requiring that section 702-acquired information subject to other destruction/age off requirements in these procedures (e.g., Section 5) be retained because it is subject to a preservation requirement. In such cases the Government will notify the Foreign Intelligence Surveillance Court and seek permission to retain the material as appropriate consistent with law. Depending on the nature, scope and complexity of a particular preservation obligation, in certain circumstances it may be technically infeasible to retain certain section 702-acquired information. Should such circumstances arise, they will be brought to the attention of the court with jurisdiction over the underlying litigation matter for resolution.

(d) (U) Change in Target's Location or Status

(1) (U//~~FOUO~~) In the event that NSA reasonably believes that a target is located outside the United States and subsequently learns that the person is inside the United States, or if NSA concludes that a target who at the time of targeting was believed to be a non-United States person is in fact a United States person at the time of acquisition, the acquisition from that person will be terminated without delay.

(2) (U) Any communications acquired through the targeting of a person who at the time of targeting was reasonably believed to be located outside the United States but is in fact located inside the United States at the time such communications were acquired, and any communications acquired by targeting a person who at the time of targeting was believed to be a non-United States person but was in fact a United States person at the time such communications were acquired, will be treated as domestic communications under these procedures.

(e) ~~(S//NF)~~ In the event that NSA seeks to use any information acquired pursuant to section 702 during a time period when there is uncertainty about the location of the target of the acquisition because the [redacted] post-tasking checks described in NSA's section 702

targeting procedures were not functioning properly, NSA will follow its internal procedures for determining whether such information may be used (including, but not limited to, in FISA applications, section 702 targeting, and disseminations). Except as necessary to assess location under this provision, NSA may not use or disclose any information acquired pursuant to section 702 during such time period unless NSA determines, based on the totality of the circumstances, that the target is reasonably believed to have been located outside the United States at the time the information was acquired. If NSA determines that the target is reasonably believed to have been located inside the United States at the time the information was acquired, such information will not be used and will be promptly destroyed.

(U) Section 4 - Acquisition and Handling - Attorney-Client Communications

(U) As soon as it becomes apparent that a communication is between a person who is known to be under criminal indictment in the United States and an attorney who represents that individual in the matter under indictment (or someone acting on behalf of the attorney), monitoring of that communication will cease and the communication will be identified as an attorney-client communication in a log maintained for that purpose. The relevant portion of the communication containing that conversation will be segregated and the National Security Division of the Department of Justice will be notified so that appropriate procedures may be established to protect such communications from review or use in any criminal prosecution, while preserving foreign intelligence information contained therein. Additionally, all proposed dissemination of information constituting United States person attorney-client privileged communications must be reviewed by the NSA Office of General Counsel prior to dissemination.

(U) Section 5 - Domestic Communications

~~(TS//SI//NF)~~ A communication identified as a domestic communication (and, if applicable, the Internet transaction in which it is contained) will be promptly destroyed upon recognition unless the Director (or Acting Director) of NSA specifically determines, in writing and on a communication-by-communication basis, that the sender or intended recipient of the domestic communication had been properly targeted under section 702 of the Act, and the domestic communication satisfies one or more of the following conditions:

(1) ~~(TS//SI//NF)~~ such domestic communication is reasonably believed to contain significant foreign intelligence information. Such domestic communication (and, if applicable, the transaction in which it is contained) may be retained, handled, and disseminated in accordance with these procedures;

(2) ~~(TS//SI//NF)~~ such domestic communication does not contain foreign intelligence information but is reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed. Such domestic communication may be disseminated (including United States person identities) to appropriate Federal law enforcement authorities, in accordance with 50 U.S.C. §§ 1806(b) and 1825(c), Executive Order No. 12333, and, where applicable, the crimes reporting procedures

set out in the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document. Such domestic communication (and, if applicable, the transaction in which it is contained) may be retained by NSA for a reasonable period of time, not to exceed six months unless extended in writing by the Attorney General, to permit law enforcement agencies to determine whether access to original recordings of such communication is required for law enforcement purposes;

(3) ~~(TS//SI//NF)~~ such domestic communication is reasonably believed to contain technical data base information, as defined in Section 2(j), or information necessary to understand or assess a communications security vulnerability. Such domestic communication may be provided to the FBI and/or disseminated to other elements of the United States Government. Such domestic communication (and, if applicable, the transaction in which it is contained) may be retained for a period sufficient to allow a thorough exploitation and to permit access to data that is, or is reasonably believed likely to become, relevant to a current or future foreign intelligence requirement. Sufficient duration may vary with the nature of the exploitation.

a. (U//~~FOUO~~) In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis.

b. ~~(S//SI~~ [redacted] In the case of communications that are not enciphered or otherwise reasonably believed to contain secret meaning, sufficient duration is five years from expiration date of the certification authorizing the collection for telephony communications and Internet communications acquired by or with the assistance of the FBI from Internet Service Providers, and two years from expiration date of the certification authorizing the collection for Internet transactions acquired through NSA's upstream collection techniques, unless the Signal Intelligence Director, NSA, determines in writing that retention of a specific communication for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements; or

(4) (U//~~FOUO~~) such domestic communication contains information pertaining to an imminent threat of serious harm to life or property. Such information may be retained and disseminated to the extent reasonably necessary to counter such threat.

~~(S//NF)~~ Notwithstanding the above, if a domestic communication indicates that a target has entered the United States, NSA may promptly notify the FBI of that fact, as well as any information concerning the target's location that is contained in the communication. NSA may also use information derived from domestic communications for collection avoidance purposes, and may provide such information to the FBI and CIA for collection avoidance purposes. NSA may retain the communication from which such information is

derived but shall restrict the further use or dissemination of the communication by placing it on the Master Purge List (MPL).

(U) Section 6 - Foreign Communications of or Concerning United States Persons

(a) (U) Retention

(U) Foreign communications of or concerning United States persons collected in the course of an acquisition authorized under section 702 of the Act may be retained only:

(1) (U) if necessary for the maintenance of technical data bases. Retention for this purpose is permitted for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future foreign intelligence requirement. Sufficient duration may vary with the nature of the exploitation.

a. (U) In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis.

b. ~~(TS//SI//NF)~~ In the case of communications that are not enciphered or otherwise reasonably believed to contain secret meaning, sufficient duration is five years from expiration date of the certification authorizing the collection for telephony communications and Internet communications acquired by or with the assistance of the FBI from Internet Service Providers, and two years from expiration date of the certification authorizing the collection for Internet transactions acquired through NSA's upstream collection techniques, unless the Signals Intelligence Director, NSA, determines in writing that retention of a specific category of communications for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements;

(2) (U) if dissemination of such communications with reference to such United States persons would be permitted under subsection (b) below; or

(3) (U) if the information is evidence of a crime that has been, is being, or is about to be committed and is provided to appropriate federal law enforcement authorities.

~~(TS//SI//NF)~~ Foreign communications of or concerning United States persons that may be retained under subsections 6(a)(2) and (3) above include discrete communications contained in Internet transactions, provided that NSA has specifically determined, consistent with subsection 3(c)(2) above, that each discrete communication within the Internet transaction either: (a) is to, from, or about a tasked selector; or (b) is not to, from, or about a tasked selector and is also not to or from an identifiable United States person or person reasonably believed to be in the United States.

(b) (U) Dissemination

(U) A dissemination based on communications of or concerning a United States person may be made in accordance with Section 7 or 8 below if the identity of the United States person is deleted and a generic term or symbol is substituted so that the information cannot reasonably be connected with an identifiable United States person. Otherwise, dissemination of intelligence based on communications of or concerning a United States person may only be made to a recipient requiring the identity of such person for the performance of official duties but only if at least one of the following criteria is also met:

(1) (U) the United States person has consented to dissemination or the information of or concerning the United States person is available publicly;

(2) (U) the identity of the United States person is necessary to understand foreign intelligence information or assess its importance, e.g., the identity of a senior official in the Executive Branch;

(3) (U) the communication or information indicates that the United States person may be:

a. an agent of a foreign power;

b. a foreign power as defined in section 101(a) of the Act;

c. residing outside the United States and holding an official position in the government or military forces of a foreign power;

d. a corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or

e. acting in collaboration with an intelligence or security service of a foreign power and the United States person has, or has had, access to classified national security information or material;

(4) (U) the communication or information indicates that the United States person may be the target of intelligence activities of a foreign power;

(5) (U) the communication or information indicates that the United States person is engaged in the unauthorized disclosure of classified national security information or the United States person's identity is necessary to understand or assess a communications or network security vulnerability, but only after the agency that originated the information certifies that it is properly classified;

(6) (U) the communication or information indicates that the United States person may be engaging in international terrorist activities;

(7) (U//~~FOUO~~) the acquisition of the United States person's communication was authorized by a court order issued pursuant to the Act and the communication may relate to the foreign intelligence purpose of the surveillance; or

(8) (U) the communication or information is reasonably believed to contain evidence that a crime has been, is being, or is about to be committed, provided that dissemination is for law enforcement purposes and is made in accordance with 50 U.S.C. §§ 1806(b) and 1825(c), Executive Order No. 12333, and, where applicable, the crimes reporting procedures set out in the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document.

(c) (U) Provision of Unminimized Communications to CIA and FBI

(1) (U) NSA may provide to the Central Intelligence Agency (CIA) unminimized communications acquired pursuant to section 702 of the Act. CIA will identify to NSA targets for which NSA may provide unminimized communications to CIA. CIA will handle any such unminimized communications received from NSA in accordance with CIA minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act.

(2) (U) NSA may provide to the FBI unminimized communications acquired pursuant to section 702 of the Act. The FBI will identify to NSA targets for which NSA may provide unminimized communications to the FBI. The FBI will handle any such unminimized communications received from NSA in accordance with FBI minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act.

(U) Section 7 - Other Foreign Communications

(U) Foreign communications of or concerning a non-United States person may be retained, used, and disseminated in any form in accordance with other applicable law, regulation, and policy.

(~~TS//SI//NF~~) Foreign communications of or concerning a non-United States person that may be retained under this subsection include discrete communications contained in Internet transactions, provided that NSA has specifically determined, consistent with subsection 3(c)(2) above, that each discrete communication within the Internet transaction either: (a) is to, from, or about a tasked selector; or (b) is not to, from, or about a tasked selector and is also not to or from an identifiable United States person or person reasonably believed to be in the United States.

(U//~~FOUO~~) Additionally, foreign communications of or concerning a non-United States person may be retained for the same purposes and in the same manner as detailed in Section 6(a)(1), above.

(U) Section 8 - Collaboration with Foreign Governments

(a) (U) Procedures for the dissemination of evaluated and minimized information. Pursuant to section 1.7(c)(8) of Executive Order No. 12333, as amended, NSA conducts foreign cryptologic liaison relationships with certain foreign governments. Information acquired pursuant to section 702 of the Act may be disseminated to a foreign government. Except as provided below in subsection 8(b) of these procedures, any dissemination to a foreign government of information of or concerning a United States person that is acquired pursuant to section 702 may only be done in a manner consistent with sections 6(b) and 7 of these NSA minimization procedures.

(b) (U) Procedures for technical or linguistic assistance. It is anticipated that NSA may obtain information or communications that, because of their technical or linguistic content, may require further analysis by foreign governments to assist NSA in determining their meaning or significance. Notwithstanding other provisions of these minimization procedures, NSA may disseminate computer disks, tape recordings, transcripts, or other information or items containing unminimized information or communications acquired pursuant to section 702 to foreign governments for further processing and analysis, under the following restrictions with respect to any materials so disseminated:

(1) (U) Dissemination to foreign governments will be solely for translation or analysis of such information or communications, and assisting foreign governments will make no use of any information or any communication of or concerning any person except to provide technical and linguistic assistance to NSA.

(2) (U) Dissemination will be only to those personnel within foreign governments involved in the translation or analysis of such information or communications. The number of such personnel will be restricted to the extent feasible. There will be no dissemination within foreign governments of this unminimized data.

(3) (U) Foreign governments will make no permanent agency record of information or communications of or concerning any person referred to or recorded on computer disks, tape recordings, transcripts, or other items disseminated by NSA to foreign governments, provided that foreign governments may maintain such temporary records as are necessary to enable them to assist NSA with the translation or analysis of such information. Records maintained by foreign governments for this purpose may not be disseminated within the foreign governments, except to personnel involved in providing technical or linguistic assistance to NSA.

(4) (U) Upon the conclusion of such technical or linguistic assistance to NSA, computer disks, tape recordings, transcripts, or other items or information disseminated to foreign governments will either be returned to NSA or be destroyed with an accounting of such destruction made to NSA.

(5) (U) Any information that foreign governments provide to NSA as a result of such technical or linguistic assistance may be disseminated by NSA in accordance with these minimization procedures.

7/24/14
Date

Eric H. Holder, Jr.
Attorney General of the United States

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, Plaintiff, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	)	Civil Action No. 1:15-cv-00662-TSE

EXHIBIT B

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, Plaintiff, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	No. 1:15-cv-00662-TSE

PUBLIC DECLARATION OF DANIEL R. COATS,
DIRECTOR OF NATIONAL INTELLIGENCE

I, DANIEL R. COATS, do hereby state and declare as follows:

INTRODUCTION

1. I am the Director of National Intelligence ("DNI") and have held this position since March 16, 2017. As the DNI, I oversee the United States Intelligence Community ("IC") and serve as the principal intelligence advisor to the President. Prior to commencing my role as the DNI, I held various positions within the United States Congress. Specifically, from 1981 to 1999, I served in the U.S. House of Representatives and then in the U.S. Senate. During this tenure, I served on the Senate Armed Services Committee and the Senate Select Committee on Intelligence where I worked to strengthen our nation's defense and security. Following my time in Congress, I was named U.S. Ambassador to the Federal Republic of Germany, where I served as the Ambassador from 2001 to 2005. As a U.S. Ambassador and Chief of Mission, I was responsible for leading the embassy's charge to ensure that U.S. foreign policy goals were advanced; the embassy served American interests and values, and all executive branch agencies attached to the embassy did likewise; and executive, legislative, and judicial responsibilities were

carried out. Further, in my role as Chief of Mission, I was directly responsible for the security of the mission, including security from terrorism and protection of all U.S. Government personnel on official duty. After my tenure as U.S. Ambassador to the Federal Republic of Germany, I returned to the U.S. Senate in 2011 and again served on the Senate Select Committee on Intelligence, where I was charged with overseeing intelligence activities and programs of the U.S. Government.

2. The position of the DNI was created by Congress in the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, §§ 1011(a) and 1097, 118 Stat. 3638, 3643-63, 3698-99 (2004) (amending sections 102 through 104 of Title I of the National Security Act of 1947). Subject to the authority, direction, and control of the President, the DNI serves as the head of the IC and as the principal adviser to the President and the National Security Council for intelligence matters related to national security. *See* 50 U.S.C. § 3023(b)(1)-(2).

3. The IC includes the Office of the Director of National Intelligence; the National Security Agency ("NSA"); the Central Intelligence Agency; the Defense Intelligence Agency; the National Geospatial-Intelligence Agency; the National Reconnaissance Office; other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs; the intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Coast Guard, the Federal Bureau of Investigation, the Drug Enforcement Administration, and the Department of Energy; the Bureau of Intelligence and Research of the Department of State; the Office of Intelligence and Analysis of the Department of the Treasury; the Office of Intelligence and Analysis of the Department of Homeland Security; and such other elements of any other department or agency as may be designated by the President, or jointly

designated by the DNI and heads of the department or agency concerned, as an element of the IC. *See* 50 U.S.C. § 3003(4); *see also* Executive Order 12333 § 3.5.

4. The National Security Act of 1947, as amended, provides that "[t]he Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure." 50 U.S.C. § 3024(i)(1). By this language, Congress expressed its determination that disclosure of intelligence sources or methods is potentially harmful to national security and directed the DNI to protect them.

5. By virtue of my position as the DNI, unless otherwise directed by the President, I have access to all intelligence related to the national security that is collected by any department, agency, or other entity of the United States. 50 U.S.C. § 3024(b).

6. I make the following statements based on my personal knowledge and on information made available to me in my official capacity. Moreover, I have read and personally considered the information contained in the *In Camera, Ex Parte* Declaration of George C. Barnes, Deputy Director, NSA, executed on April 24, 2018 (hereinafter "Classified NSA Declaration").

7. In the course of my official duties, I have been advised of the above-captioned lawsuit and the allegations by the plaintiff, Wikimedia Foundation ("Wikimedia"), concerning NSA's "Upstream" surveillance, a technique employed by the NSA to gather foreign intelligence information under section 702 of the Foreign Intelligence Surveillance Act ("FISA"). I have also been advised of Wikimedia's motion to compel the Government to disclose certain documents and information responsive to Wikimedia's discovery requests ("Motion to Compel"). The purpose of this declaration is to formally assert, in my capacity as DNI and head of the IC, the state secrets privilege and my statutory privilege under the National Security Act in order to

protect intelligence information, sources, and methods that are at risk of disclosure in this case as a result of Wikimedia's Motion to Compel. *See* 50 U.S.C. § 3024(i)(1). This assertion of privilege is over highly sensitive and classified national security information concerning NSA's Upstream surveillance and falling within the categories described herein. This information must be protected because its disclosure reasonably could be expected to cause serious damage, and in many cases exceptionally grave damage, to the national security of the United States.

SUMMARY

8. As detailed in this declaration and in the Classified NSA Declaration, disclosure of the documents and information that Wikimedia seeks to compel the Government to disclose reasonably could be expected to cause serious damage, and in many cases exceptionally grave damage, to the national security of the United States. This information should be protected from disclosure to Wikimedia and excluded from any use in this case.

9. Accordingly, as set forth further below, I am asserting the state secrets privilege and the DNI's statutory authority to protect intelligence sources and methods pursuant to 50 U.S.C. § 3024(i)(1) to protect against the disclosure of highly classified and important intelligence information, sources, and methods regarding Upstream surveillance that Wikimedia has sought to compel the Government to disclose in response to Wikimedia's discovery requests (and certain deposition questions) and in response to any further discovery requests Wikimedia may serve in this case, or as otherwise may be necessary to litigate Wikimedia's claims or the Government's defenses in this case. Such information is vital to the national security of the United States and covers the following seven categories: (A) information that would tend to confirm what individuals or entities are subject to Upstream surveillance activities; (B) information concerning the operational details of the Upstream collection process; (C) the

location(s) at which Upstream surveillance is conducted; (D) the categories of Internet-based communications collected through Upstream surveillance activities; (E) information concerning the scope and scale of Upstream surveillance; (F) NSA cryptanalytic capabilities; and (G) additional categories of classified information regarding Upstream surveillance contained in opinions and orders issued by, and submissions made to, the Foreign Intelligence Surveillance Court ("FISC").

10. I make these assertions of privilege mindful of the public disclosures—both authorized and unauthorized—of information about classified NSA intelligence programs, including the IC's declassification and public release of certain materials concerning NSA's Upstream surveillance, which is the program that is challenged in this lawsuit. However, it has remained necessary to withhold considerable details about Upstream surveillance, even from publicly released documents, to protect highly sensitive intelligence information, sources and methods, such as particular subjects of surveillance and methods of collecting and analyzing intelligence information. Therefore, notwithstanding prior disclosures, it is my judgment that additional disclosure of the highly sensitive and still-classified documents and information that Wikimedia has sought to compel the Government to disclose in this case would cause serious damage, and in many cases exceptionally grave damage, to the national security of the United States.

11. Furthermore, my assertions of privilege have not been made to conceal a violation of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency of the Government; to restrain competition; or to prevent or delay the release of information that does not require protection in the interests of national security.

12. For these reasons, as set forth further below, I request that the Court uphold the state secrets and statutory privilege assertions that I make herein, as well as the statutory privilege assertion made by the NSA pursuant to Section 6 of the National Security Agency Act (50 U.S.C. § 3605(a)), and protect from disclosure the information that Wikimedia now seeks to compel the Government to disclose.

BACKGROUND OF THE CHALLENGED UPSTREAM PROGRAM

13. In July 2008, Congress enacted the Foreign Intelligence Surveillance Act Amendments Act of 2008, Pub. L. 110-261, 122 Stat. 2436. This Act added a new section 702 to FISA, 50 U.S.C. § 1881a ("Section 702"), which created new statutory authority permitting the targeting of non-United States persons reasonably believed to be outside of the United States to acquire foreign intelligence information, without individualized orders or warrants from the FISC. More specifically, Section 702 provides that, upon the FISC's approval of a "certification" submitted by the Government, the Attorney General and the DNI may jointly authorize, for up to one year, the "targeting of [non-U.S.] persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. § 1881a(a), (h). Although the statute does not require the IC to identify the specific facilities, places, premises, or property at which an authorized acquisition will be directed, the Government must certify that an acquisition involves obtaining foreign intelligence information "from or with the assistance of an electronic communication service provider." *Id.* § 1881a(h)(2)(A)(vi).

14. Under Section 702, the Attorney General and the DNI submit annual certifications to the FISC for its approval, as required under the statute, to authorize the targeting of non-U.S. persons reasonably believed to be located outside of the United States to acquire foreign

intelligence information. These certifications identify categories of foreign intelligence information authorized for acquisition but do not identify the particular non-U.S. persons who will be targeted. Instead, the certifications include targeting procedures, approved by the Attorney General in consultation with the DNI, which must, among other things, be reasonably designed to ensure that any Section 702 acquisition is limited to targeting persons reasonably believed to be located outside the United States, and to prevent the intentional acquisition of wholly domestic communications. In addition, the targeting procedures specify the manner in which the IC determines whether a person is a non-U.S. person reasonably believed to be located outside the United States who is likely to possess or receive foreign intelligence information authorized for acquisition by a certification.[1]

15. There are two types of Section 702 acquisition: what has been publicly referred to as "PRISM" collection and "Upstream" collection. I understand that this case involves a legal challenge to Upstream collection. In unclassified terms, in the course of the Upstream collection process, certain Internet transactions transiting the Internet backbone network(s) of certain electronic communication service provider(s) are filtered for the purpose of excluding wholly domestic communications and are then scanned to identify for acquisition those transactions that

1. Four requirements must be met for FISC approval of a Section 702 certification. First, the Attorney General and the DNI must certify, among other things, that a significant purpose of the acquisitions is to obtain foreign intelligence information, as that term is defined under FISA, and the FISC must find that the Attorney General and DNI's certification contains all of the required statutory elements. 50 U.S.C. § 1881a(h)(2)(A)(v), (j)(2)(A). Second, the FISC must find that the Government's targeting procedures are reasonably designed to ensure that acquisitions conducted under the authorization (a) are limited to targeting non-U.S. persons reasonably believed to be located outside the United States, and (b) will not intentionally acquire communications known at the time of acquisition to be purely domestic. *Id.* § 1881a(j)(2)(B). Third, the FISC must find that the Government's minimization procedures meet FISA's requirements. *Id.* §§ 1801(h), 1821(4), 1881a(j)(2)(C). And fourth, the FISC must find that the Government's targeting and minimization procedures are consistent, not only with FISA, but also with the requirements of the Fourth Amendment. *Id.* § 1881a(j)(3)(A). Following passage of the FISA Amendments Reauthorization Act of 2017, the FISC must now also find that the Government's querying procedures meet the statutory requirements and are consistent with the Fourth Amendment. *Id.* § 1881a(j)(2)(D); (j)(3)(A).

are to or from (or, prior to early 2017, to, from, or "about") persons[2] targeted in accordance with the applicable NSA targeting procedures; only those transactions that pass through both the filtering and the scanning are ingested into Government databases. While the Upstream collection process has been described in general terms in this declaration and in declassified documents and unclassified reports, certain operational details of Upstream collection remain highly classified as described in the Classified NSA Declaration.

ASSERTION OF THE STATE SECRETS PRIVILEGE

16. After careful and actual personal consideration of the matter, based upon my own knowledge and on information obtained in the course of my official duties, including the information contained in the Classified NSA Declaration, I have determined that Wikimedia's Motion to Compel implicates highly sensitive and classified state secrets concerning intelligence information, sources, and methods. Disclosure of such information—as set forth herein and described in more detail in the Classified NSA Declaration—reasonably could be expected to cause serious damage, and in many cases exceptionally grave damage, to the national security of the United States. This information must be protected from disclosure and excluded from use in this case. Therefore, as to the information Wikimedia seeks to compel the Government to disclose, I formally assert the state secrets privilege.

ASSERTION OF STATUTORY PRIVILEGE UNDER NATIONAL SECURITY ACT

17. Through this declaration, I also hereby invoke and assert a statutory privilege held by the DNI under the National Security Act of 1947, as amended, to protect the information described herein and in the Classified NSA Declaration, *see* 50 U.S.C. § 3024(i)(1). My

2. When the NSA targets a non-U.S. person under Section 702, it must identify a specific communications identifier, known as a "selector." A selector cannot be the name of the individual or a keyword.

assertion of this statutory privilege for intelligence sources and methods is coextensive with my state secrets privilege assertion.

INFORMATION SUBJECT TO ASSERTIONS OF PRIVILEGE

18. In general and unclassified terms, documents and information responsive to Wikimedia's discovery requests that Wikimedia has sought to compel the Government to disclose are subject to my state secrets and statutory privilege assertions because they contain the following seven categories of classified information:

A. *Individuals or Entities Subject to Upstream Surveillance Activities:* Documents and information responsive to Wikimedia's pending discovery requests, to any future discovery that Wikimedia may seek, or that may otherwise be necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this litigation, that indicate or may tend to indicate whether communications of Wikimedia, and/or of other individuals and entities, have been subject to Upstream surveillance activities;

B. *Operational Details of the Upstream Collection Process:* Documents and information (not already encompassed by other categories herein) responsive to Wikimedia's pending discovery requests or to any future discovery that Wikimedia may seek, or that may otherwise be necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this litigation, that reveal or may tend to reveal still-classified technical details concerning the methods, processes, and devices employed (including the design, operation, and capabilities of the devices employed) to conduct Upstream surveillance;

C. *Location(s) at Which Upstream Surveillance is Conducted:* Documents and information responsive to Wikimedia's pending discovery requests, to any future discovery that Wikimedia may seek, or that may otherwise be necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this litigation, that reveal or may tend to reveal still-classified information about any specific location(s), or the nature of the location(s), on the Internet backbone network(s) of U.S. electronic communication service provider(s) at which Upstream surveillance is conducted;

D. *Categories of Internet-Based Communications Subject to Upstream Surveillance Activities:* Documents and information responsive to Wikimedia's pending discovery requests, to any future discovery that Wikimedia may seek, or that may otherwise be necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this litigation, that reveal or may tend to reveal still-classified information about the specific types or categories of communications either subject to or acquired in the course of the Upstream collection process;

E. *Scope and Scale on Which Upstream Surveillance Is or Has Been Conducted:* Documents and information responsive to Wikimedia's pending discovery requests, to any future discovery that Wikimedia may seek, or that may otherwise be necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this litigation, that reveal or may tend to reveal still-classified information about (i) the volume or proportion of Internet communications traffic, including international Internet communications, either subject to or acquired in the course of the Upstream collection process, (ii) the number, proportion, and/or bandwidth of any circuit, international submarine or terrestrial cable, or other Internet backbone link, on which Upstream surveillance is or has been conducted; and (iii) any other measure of the scope or scale on which Upstream surveillance is or has been conducted;

F. *NSA Cryptanalytic Capabilities (or Lack Thereof)*: Documents and information responsive to Wikimedia's pending discovery requests, to any future discovery that Wikimedia may seek, or that may otherwise be necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this litigation, that reveal or may tend to reveal still-classified information about the NSA's capability, or lack thereof, to decrypt, circumvent, or defeat specific types of communications security protocols; and

G. *Additional Categories of Classified Information Contained in Opinions and Orders issued by, and submissions made to, the FISC Concerning Upstream:* The additional categories of classified information contained in the documents responsive to Wikimedia's discovery Requests for Production numbered 21 and 22 (and not already encompassed by categories A-F, above) as set forth in the privilege log served by Defendant United States Department of Justice on March 19, 2018.

HARM OF DISCLOSING INFORMATION SUBJECT TO PRIVILEGE

19. As discussed in detail in the Classified NSA Declaration, protection of these categories of information is key to the NSA's ability to produce foreign intelligence information, which depends on its access to foreign and international electronic communications. Foreign intelligence information produced by communications intelligence activities, such as Upstream surveillance, is an extremely important part of the overall foreign intelligence information available to the United States. Indeed, communications intelligence is often the only means by which the United States can learn the existence of particular threats or the identities of particular individuals who are involved in hostile activities. Communications intelligence is thus essential to the ability of the IC to identify adversaries and to detect and disrupt their plans for attacks and other hostile acts against the United States. Against that backdrop, the risks of disclosing the specific categories of information described herein are especially grave.

20. Below, I describe each of these categories, and the harm that reasonably could be expected to result from disclosure, in unclassified terms. Much of the harm, however, necessarily must be described in classified terms, and, as such, is set forth in the Classified NSA Declaration.

A. Information That May Tend to Confirm or Deny Whether or Not the Communications of Wikimedia or Other Individuals or Entities Have Been Subjected to Upstream Surveillance Activities.

21. The first category of information over which I am asserting privilege is information that would tend to reveal whether particular individuals or entities, including Wikimedia, have been subjected to Upstream surveillance activities. Disclosure of such information reasonably could be expected to cause exceptionally grave damage to the national security of the United States.

22. My privilege assertion over information that may tend to confirm or deny whether or not the communications of Wikimedia, or other individuals or entities, have been subject to Upstream surveillance includes, for example, Wikimedia's attempt to compel the Government to confirm or deny whether or not NSA has copied, reviewed the content of, and/or retained at least one Wikimedia communication in the course of Upstream surveillance, and Wikimedia's attempt to compel the Government to confirm or deny the authenticity of purportedly classified documents which Wikimedia believes indicate that the NSA targets its communications for Upstream surveillance.

23. The Government cannot publicly confirm or deny whether any particular individual or entity is subject to intelligence-gathering activities, no matter how likely or unlikely it might appear that the individual or entity would be subject to surveillance. If the Government were to reveal that an individual or entity is the target or a subject of intelligence-gathering, the collection capability relating to that individual or entity would certainly be compromised. On the other hand, if the Government were to reveal that an individual or entity is not the target or subject of intelligence-gathering, adversaries would know that a particular individual has avoided scrutiny and is a secure source for communicating. Moreover, providing assurances to those individuals who (or entities which) are not targets or subjects quickly becomes unworkable when faced with a situation in which an individual (or entity) has in fact been a target or subject. If the Government were to confirm that any specific individual or entity is not a target or subject of intelligence-gathering, but later refuse to confirm or deny that fact in a situation involving an actual target or subject, it would be apparent that intelligence-gathering was occurring in the latter case. The only recourse for the Government is to neither confirm nor deny whether someone (or some entity) has been targeted by or subject to NSA intelligence-gathering

activities, regardless of whether the individual or entity has been a target or subject or not. To say otherwise when challenged in litigation would result in the frequent, routine exposure of intelligence information, sources, and methods, and would severely undermine surveillance activities in general.

24. After personal consideration of the matter, it is my judgment that disclosing the information described herein (and in further detail in the Classified NSA Declaration) would compromise important and critical information, sources, and methods, causing exceptionally grave damage to the national security of the United States.

B. Operational Details of the Upstream Collection Process.

25. The second category of information over which I am asserting privilege is still-classified information concerning the operational details of the Upstream collection process, as discussed in greater detail in the Classified NSA Declaration (and where such information is not already encompassed by other categories of privileged information described elsewhere in this declaration). Public disclosure of such information reasonably could be expected to cause exceptionally grave damage to the national security of the United States.

26. My privilege assertion over the operational details of the Upstream collection process includes, for example, Wikimedia's request for additional technical details concerning "filtering mechanisms" employed by NSA and the "scanning," "screening," and content review of communications during Upstream surveillance. Although the IC has publicly acknowledged the existence of the Upstream surveillance program and has publicly released a limited amount of information describing, at a high level of generality, how Upstream operates, additional technical details about the Upstream collection process remain classified.

27. As discussed in greater detail in the Classified NSA Declaration, disclosure of still-classified operational details regarding Upstream surveillance, either directly or indirectly, would reveal to our adversaries the extent of the ability of the United States to monitor and track their activities and communications, thereby helping our adversaries evade detection, which would seriously compromise, if not destroy, important and vital ongoing intelligence operations.

28. After personal consideration of the matter, it is my judgment that disclosing the information described herein (and in further detail in the Classified NSA Declaration) would compromise important and critical information, sources, and methods, causing exceptionally grave damage to the national security of the United States.

C. The Location(s) Where Upstream Surveillance is Conducted.

29. The third category of information over which I am asserting privilege is information that would, directly or indirectly, tend to reveal the location(s) on the Internet backbone where Upstream surveillance is conducted. Public disclosure of such information, even at a general level, reasonably could be expected to cause exceptionally grave damage to the national security of the United States.

30. My privilege assertion over the location(s) on the Internet backbone where Upstream surveillance is conducted includes information regarding the number and nature of such Upstream surveillance point(s). For example, Wikimedia has sought disclosure of information sufficient to show the "number of circuits" and "number of Internet chokepoints" at which Upstream surveillance is conducted. Although the IC has publicly acknowledged that Upstream surveillance is conducted on one or more points on the Internet backbone, we have not acknowledged any further details regarding the location of these one or more points or any information about the nature or number of these one or more points.

31. As discussed in greater detail in the Classified NSA Declaration, disclosing information on the location(s) where Upstream surveillance is conducted would assist foreign adversaries in trying to evade particular channels of communications that are being monitored, exploit any particular channels of communications that are not being monitored, and target location(s) where the NSA obtains critical foreign intelligence information for hostile action.

32. After personal consideration of the matter, it is my judgment that disclosing the information described herein (and in further detail in the Classified NSA Declaration), either directly or indirectly, would compromise important and critical information, sources, and methods, causing exceptionally grave damage to the national security of the United States.

D. Categories of Internet-Based Communications Subject to Upstream Surveillance Activities.

33. The fourth category of information over which I am asserting privilege is information that would tend to reveal categories of Internet-based communications subject to and not subject to Upstream surveillance activities. Public disclosure of such information reasonably could be expected to cause exceptionally grave damage to the national security of the United States.

34. My privilege assertion over information that would tend to reveal the types of communications collected through Upstream surveillance includes, for example, information sought by Wikimedia in deposition questions it asked NSA's designated witness concerning whether NSA collection devices are configured to exclude various types of encrypted communications. However, as discussed in greater detail in the Classified NSA Declaration, disclosing information on the types of communications collected through Upstream surveillance would induce our foreign adversaries to avoid those forms of online communications in order to defeat NSA's attempts to capture their communications.

35. After personal consideration of the matter, it is my judgment that disclosing the information described herein (and in further detail in the Classified NSA Declaration) would compromise important and critical information, sources, and methods, causing exceptionally grave damage to the national security of the United States.

E. Information Concerning the Scope and Scale of Upstream Surveillance.

36. The fifth category of information over which I am asserting privilege is information concerning the scope and scale of Upstream surveillance. Public disclosure of such information reasonably could be expected to cause exceptionally grave damage to the national security of the United States.

37. My privilege assertion over the scope and scale of Upstream surveillance includes, for example, Wikimedia's requests that the Government describe the approximate amount of Internet traffic subject to each stage of the Upstream collection process and that the Government admit that the NSA conducts Upstream surveillance on "multiple international Internet links." The IC has publicly acknowledged that (a) NSA is monitoring at least one circuit carrying international Internet communications and (b) the Upstream process necessarily involves the NSA having access to a larger body of communications than those that contain the targeted selectors in order to filter and scan that larger body to ingest into NSA repositories only those communications containing the selectors. However, any additional facts about the scope and scale of the Upstream surveillance program remain classified.

38. As discussed in greater detail in the Classified NSA Declaration, disclosing information regarding the scope and scale of Upstream surveillance would inform foreign adversaries whether they should increase or decrease their efforts to avoid such surveillance.

39. After personal consideration of the matter, it is my judgment that disclosing the information described herein (and in further detail in the Classified NSA Declaration) would compromise important and critical information, sources, and methods, causing exceptionally grave damage to the national security of the United States.

F. NSA Cryptanalytic Capabilities (or Lack Thereof).

40. The sixth category of information over which I am asserting privilege is information concerning NSA's capabilities, or lack thereof, to decrypt, circumvent, or defeat communications security protocols. Public disclosure of such information reasonably could be expected to cause exceptionally grave damage to the national security of the United States.

41. My privilege assertion over the NSA's cryptanalytic capabilities includes, for example, Wikimedia's request that the Government describe any Internet Protocols subject to Upstream surveillance that NSA is able to decrypt, as well as Wikimedia's request that the Government admit whether NSA has the ability to decrypt any portion of HTTPS (HyperText Transfer Protocol Secure) communications that may be subject to Upstream surveillance.

42. As discussed in greater detail in the Classified NSA Declaration, NSA's capabilities against communications security protocols are exceptionally fragile. Public disclosure of information concerning NSA's capabilities, or lack thereof, to decrypt, circumvent, or defeat communications security protocols would cause adversaries to shift their communications to less susceptible protocols. NSA's resulting loss of foreign intelligence information would cause irreparable damage to national security.

43. After personal consideration of the matter, it is my judgment that disclosing the information described herein (and in further detail in the Classified NSA Declaration) would

compromise important and critical information, sources, and methods, causing exceptionally grave damage to the national security of the United States.

G. Additional Categories of Classified Information Contained in Opinions and Orders Issued by, and Submissions Made to, the FISC Concerning Upstream Surveillance.

44. Finally, the seventh category of information over which I am asserting privilege is information contained in opinions and orders issued by, and submissions made to, the FISC concerning Upstream surveillance (where such information is not already encompassed by other categories of privileged information described elsewhere in this declaration). Public disclosure of such information reasonably could be expected to cause exceptionally grave damage to the national security of the United States.

45. My privilege assertion over information contained within opinions and orders issued by, and submissions made to, the FISC concerning Upstream surveillance stems from Wikimedia's request that the Government produce every such opinion, order, or submission concerning Upstream surveillance in its entirety. Although the IC has already publicly released some of these documents in redacted form—including a release of significant FISC opinions concerning FISA Section 702—additional information in these documents remains classified.

46. Because Wikimedia has nonetheless sought disclosure of every opinion, order, and submission concerning Upstream, its expansive request necessarily implicates multiple categories of information, which cannot be described further on the public record but are set forth in the Classified NSA Declaration. The release of this information would be devastating to NSA's mission and collection efforts pursuant to Upstream surveillance, as described in the Classified NSA Declaration.

47. After personal consideration of the matter, it is my judgment that disclosing the information described herein (and in further detail in the Classified NSA Declaration) would

compromise important and critical information, sources, and methods, causing serious damage, and in many cases exceptionally grave damage, to the national security of the United States.

CONCLUSION

48. In sum, I am asserting the state secrets privilege and the DNI's statutory privilege set forth in 50 U.S.C. § 3024(i)(1) to protect classified documents and information regarding Upstream surveillance that Wikimedia has sought to compel the Government to disclose in response to Wikimedia's discovery requests (and certain deposition questions), as well as in response to any further discovery requests Wikimedia may serve in this case, or as otherwise may be necessary to litigate Wikimedia's claims or the Government's defenses in this case. I have set forth, in general and unclassified terms, as much as I can say on the public record concerning the highly sensitive and classified intelligence information, sources, and methods covered by my privilege assertions and the harm that would result from their disclosure; for a more detailed, classified description of such information, I respectfully refer the Court to the Classified NSA Declaration.

49. I respectfully request that the Court take all steps necessary to protect the intelligence information, sources, and methods described herein in order to prevent serious damage, and in many cases exceptionally grave damage, to the national security of the United States.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on: April 25, 2018

DANIEL R. COATS
Director of National Intelligence

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, Plaintiff, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	)	Civil Action No. 1:15-cv-00662-TSE

EXHIBIT C

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, Plaintiff, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	Civil Action No. 1:15-cv-00662-TSE

DECLARATION OF LAUREN L. BERNICK

I, Lauren L. Bernick, do hereby state and declare as follows:

I. Introduction

1. I am a Senior Associate Civil Liberties Protection Officer in the Office of Civil Liberties, Privacy, and Transparency ("CLPT") at the Office of the Director of National Intelligence ("ODNI"). I have held this supervisory position since August 8, 2017. Prior to my current position, I was assigned to the ODNI's CLPT office as an Associate, and then a Senior Associate, Civil Liberties Protection Officer on a temporary "detail" assignment from the National Security Division of the Department of Justice ("DOJ"). At DOJ, I served as an attorney-advisor in the Office of Intelligence handling issues related to the Foreign Intelligence Surveillance Act ("FISA"), including the drafting of FISA applications and litigating before the Foreign Intelligence Surveillance Court ("FISC"), from February 2004 until my detail assignment to ODNI in June 2013.

2. CLPT's mission is, among other things, to ensure that the Intelligence Community ("IC")[1] carries out its national security mission in a manner that protects privacy and

1. The IC is comprised of ODNI; the Central Intelligence Agency; the National Security Agency; the Defense Intelligence Agency; the National Geospatial-Intelligence Agency; the National Reconnaissance Office; other

civil liberties and provides appropriate transparency to the public in accordance with the *Principles of Intelligence Transparency for the Intelligence Community* (hereinafter, "*Transparency Principles*").[2] *See* ODNI, *Intelligence Community Directive 107* (2018), https://www.dni.gov/files/documents/ICD/ICD-107.pdf. The Chief of the CLPT office also serves as the ODNI's Chief Transparency Officer. *Id*. To fulfill its transparency mission, CLPT's subject matter expertise includes national security laws (e.g., FISA); classification of national security information; and the processes required to effectuate classification and the authorized released of unclassified information.

3. As part of my current and past duties with CLPT, I am responsible for participating in the oversight of the IC's implementation of Section 702 of FISA.[3] Specifically, the Director of National Intelligence ("DNI") has a statutory duty to assess the IC elements' compliance with procedures and guidelines promulgated pursuant to Section 702. *See* 50 U.S.C. § 1881a(m)(1). The IC elements that currently implement Section 702 are the National Security Agency ("NSA"); Central Intelligence Agency ("CIA"); Federal Bureau of Investigation ("FBI"); and ODNI's National Counterterrorism Center ("NCTC"). I am also responsible for promoting the authorized release of FISA information as it comports with the *Transparency*

---

offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs; the intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Coast Guard, the Federal Bureau of Investigation, the Drug Enforcement Administration, and the Department of Energy; the Bureau of Intelligence and Research of the Department of State; the Office of Intelligence and Analysis of the Department of the Treasury; the Office of Intelligence and Analysis of the Department of Homeland Security; and such other elements of any other department or agency as may be designated by the President, or jointly designated by the DNI and heads of the department or agency concerned, as an element of the IC. *See* 50 U.S.C. § 3003(4).

2. The IC's *Transparency Principles* are intended to facilitate IC decisions on making information publicly available in a manner that enhances public understanding of intelligence activities, while continuing to protect information when disclosure would harm national security. *See* ODNI, *Transparency Principles* (2015), https://www.dni.gov/files/documents/ppd-28/FINAL%20Transparency_poster%20v1.pdf.

3. Under Section 702, the Director of National Intelligence and the Attorney General may jointly authorize, for up to one year, the targeting of non-United States person reasonably believed to be located outside the United States to acquire foreign intelligence information. *See* 50 U.S.C. § 1881a.

Principles and the USA FREEDOM Act (*see* 50 U.S.C. § 1872),[4] as well as the protection of national security information as required by Executive Order 13526.

4. My subject matter expertise focuses on FISA, in particular Section 702. I have developed this expertise through my participation in the following tasks while working at ODNI and DOJ: drafting the joint DNI and Attorney General report assessing the IC elements' compliance with procedures and guidelines promulgated pursuant to Section 702; facilitating review of FISA materials, both within ODNI and among the relevant IC elements, in preparation for authorized release to the public pursuant to the IC's *Transparency Principles*; participating in the interagency classification review process of certain decisions, orders, and opinions issued by the FISC on or after the 2015 enactment of the USA FREEDOM Act; the public reporting of certain statistics relating to national security authorities, such as FISA; processing of FISA materials (including Section 702 materials) through Freedom of Information Act ("FOIA") requests and litigation; intra- and inter-agency coordination of public statements and other public education documents associated with the authorized release of FISA documents, including documents related to Section 702. As a result of these efforts, I developed expertise concerning what aspects of FISA information, and in particular Section 702 information, are and are not classified.

5. In the course of my official duties, I have been advised of the above-captioned lawsuit and the allegations by the plaintiff, Wikimedia Foundation, challenging the NSA's "Upstream" surveillance program conducted pursuant to Section 702 of FISA. I have also been advised of plaintiff's motion to compel the Government to disclose documents, including documents responsive to the following two discovery requests:

---

4. The USA FREEDOM Act added section 602 to FISA, which required the DNI, in consultation with the Attorney General, to conduct a declassification review of each decision, order, or opinion issued by the FISC that includes a significant construction or interpretation of any provision of law. *See* 50 U.S.C. § 1872.

REQUEST FOR PRODUCTION NO. 21: All Foreign Intelligence Court, Foreign Intelligence Surveillance Court of Review, and Supreme Court orders and opinions CONCERNING Upstream surveillance.

REQUEST FOR PRODUCTION NO. 22: All Foreign Intelligence Surveillance Court, Foreign Intelligence Surveillance Court of Review, and Supreme Court submissions CONCERNING Upstream surveillance.

6. I make the following statements based on my personal knowledge and on information made available to me in my official capacity. The purpose of this declaration is to advise the Court of the time, effort, and resources that would be required if the Court were to direct the IC to conduct a classification review for authorized release of all of the documents responsive to these two discovery requests.

II. Summary

7. Ordering the IC to process all of the documents responsive to these two discovery requests would require the IC to undergo a time-consuming and resource-intensive classification review process of classified FISC orders and opinions, as well as classified submissions to that court, which are estimated to total more than 10,000 pages. While it is extremely difficult to predict how long such a process would take, I can state that, in a recent FOIA case, it took the IC one year to complete the processing of approximately 80 FISC orders, opinions, and decisions, which contained less than 800 pages. *See Elec. Frontier Found. v. DOJ*, 16-cv-2041 (N.D. Cal.) ("*EFF* FOIA case"). The processing of all documents responsive to these two discovery requests is likely to take much longer given that the number of pages of classified information at issue here is more than twelve times the number involved in the *EFF* FOIA case.

III. The Requirements That Would Be Placed on the IC to Process These Two Discovery Requests

8. In the event the Court orders the Government to produce the unclassified portions of the classified documents responsive to the two discovery requests, the IC would need to conduct a classification review of more than 10,000 pages. The classification review of classified documents is extremely time consuming and resource intensive.

9. This is so for several reasons. First, the classification review will not be a generalized "pass/fail" review to determine whether a document as a whole is classified or not; instead, such a review will involve a line-by-line and word-by-word analysis to determine whether the information in each document must remain classified in accordance with applicable classification guidance and, consequently, be withheld from the public. Such a classification review will require comprehensive and consistent analysis of the sensitivities of the information, accurate application of classification guidance, and the precise use of redactions to protect all currently classified information. This process is complex and time-consuming because each redaction applied to classified information must correspond to the applicable classification guidance based on the topic and context of the individual information as well as consideration of whether the information is classified when combined with already officially released information.

10. Second, the classification review of all responsive documents will also entail determining whether any of the documents have previously been officially released in part. If any responsive document has previously been officially released in redacted form, the IC will have to determine whether those redactions remain appropriate in light of any official disclosures that may have occurred since the document was released. And, if the document itself has not been previously officially released in any form, the IC will have to determine whether any information contained in the document nevertheless already has been officially disclosed

through, for example, FOIA document productions, transparency disclosures, disclosures mandated by the USA FREEDOM Act, or various Government reports such as those issued by the NSA's Civil Liberties and Privacy Office or the Privacy and Civil Liberties Oversight Board.

11. Third, the classification review will involve multi-layered review by each applicable IC element. Each IC element has multiple internal stakeholders, such as FISA compliance officers, General Counsel offices, privacy and civil liberties offices, and classification offices, each of which may need to be consulted as part of the internal review of any particular document.

12. Finally, for each document, the classification review process will need to be coordinated among each IC element identified as possessing an equity in that document. This consultation necessarily takes time. As I stated above, the IC elements that currently implement Section 702 of FISA are the NSA, the CIA, the FBI, and NCTC. This means that, for any particular document, one or more of these equity holders will need to review every responsive document line-by-line. And, for submissions made by DOJ to the FISC, DOJ officials will also need to review those documents. Coordination between and among all of these equity holders takes time to ensure internal consistency within a document, consistency within a set of responsive documents, and consistency with documents and information previously officially disclosed.

13. If the Court orders the Government to produce the unclassified portions of the classified documents responsive to the two discovery requests, this extremely time-consuming and resource-intensive classification review process would be imposed upon a limited number of subject matter experts who have the necessary and appropriate training and experience to conduct such a review. Classification review for most of these subject matter experts is a collateral duty. These experts have significant competing priorities and responsibilities in their

respective IC elements that include, for example, supporting the operational and mission needs of their respective IC element; preparing statutorily mandated reports to Congress and transparency reports; supporting criminal and military commission cases; and handling FOIA requests and FOIA litigation. The most important of these responsibilities—supporting operational work— takes precedence over other duties. Therefore, imposing the additional duty of an onerous classification review of more than 10,000 pages will necessarily require the IC to reallocate resources from these competing priorities to the classification review, adversely affecting operational and other mission needs.

14. For all of the reasons described above, it is extremely difficult to predict the exact amount of time needed to conduct a classification review. Typically, it is not until the process has run its course that an accurate determination can be made as to the difficulty of a review. Nevertheless, I have recent experience with a similar kind of classification process that should serve as a guidepost for the Court as to the time likely required to complete the review Plaintiff seeks here. In the *EFF* FOIA case, the IC conducted a review of approximately 80 FISC orders, opinions, and decisions; about half of the documents were released in redacted form while the remainder were withheld in full. That process took one year. Less than 800 pages were at issue in that review, which is far less than the over 10,000 pages sought by plaintiff in the two discovery requests discussed herein. While it is unlikely that the review sought here would take more than a decade, a twelve-fold increase in the pages at issue means that, at the very least, the classification review Plaintiff seeks here would take more than one year, and possibly several years, to complete. The only way to reduce processing time would be for each respective IC element to divert significant resources away from operational tasks and other mission needs to process these documents.

15. While my understanding is that the Plaintiff has not narrowed its two discovery requests to seek only those documents that have not been previously subject to classification review, I can state that if such a narrowing of the requests were to be made, it would not significantly affect the processing time for all responsive documents. This is primarily because the bulk of documents responsive to these two requests are submissions to the FISC, the vast majority of which have not been previously subject to classification review. If Plaintiff were to withdraw Request for Production No. 22, and narrow Request for Production No. 21 by limiting it to solely those orders and opinions that have not been previously subject to classification review, only then would the drain on IC resources be significantly eased.

16. In sum, based on my experience in conducting classification reviews in the context of FOIA cases, transparency initiatives, and as part of the mandatory classification process established by the USA FREEDOM Act, I estimate that a court order requiring the IC to conduct a classification review of more than 10,000 pages of classified materials would take at least one year and could take several years to complete.

17. Pursuant to 28 U.S.C. § 1746, I certify under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Executed this 27th day of April, 2018.

Lauren L. Bernick
Senior Associate Civil Liberties Protection Officer
Office of the Director of National Intelligence

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, Plaintiff, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	Civil Action No. 1:15-cv-00662-TSE

NOTICE OF FILING OF UNCLASSIFIED (REDACTED) VERSION OF CLASSIFIED DECLARATION LODGED WITH THE COURT *IN CAMERA* AND *EX PARTE* ON APRIL 27, 2018, IN SUPPORT OF THE GOVERNMENT'S ASSERTION OF THE STATE SECRETS PRIVILEGE AND RELATED STATUTORY PRIVILEGES

Defendants National Security Agency ("NSA"); the United States Department of Justice; the Office of the Director of National Intelligence; General Paul M. Nakasone, in his official capacity as Director of the NSA; Jefferson B. Sessions, III, in his official capacity as Attorney General of the United States; and the Honorable Daniel Coats, in his official capacity as Director of National Intelligence, hereby give notice that they are filing, as an attachment hereto, a redacted, unclassified version of the Classified Declaration of George C. Barnes, Deputy Director of the NSA, which was lodged with the Court Information Security Officer on April 27, 2018, for the Court's *in camera*, *ex parte* consideration in support of the Government's assertion in this matter of the state secrets privilege and the statutory privileges established under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a). *See* ECF No. 137 (notice of lodging of Classified Declaration of George C. Barnes, Deputy Director of the NSA).

Dated: May 11, 2018

Respectfully submitted,

CHAD A. READLER
Acting Assistant Attorney General

ANTHONY J. COPPOLINO
Deputy Branch Director

/s/ James J. Gilligan
JAMES J. GILLIGAN
Special Litigation Counsel

RODNEY PATTON
Senior Trial Counsel

JULIA A. BERMAN
TIMOTHY A. JOHNSON
OLIVIA HUSSEY-SCOTT
Trial Attorneys

U.S Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave., N.W., Room 6102
Washington, D.C. 20001
Phone: (202) 514-3358
Fax: (202) 616-8470
james.gilligan@usdoj.gov

Counsel for Defendants

ATTACHMENT

~~TOP SECRET//SI//ORCON/NOFORN~~

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION,	)	
Plaintiff,	)	
v.	)	No. 1:15-cv-00662-TSE
NATIONAL SECURITY AGENCY, *et al.*,	)	
Defendants	)	

CLASSIFIED DECLARATION OF GEORGE C. BARNES,
DEPUTY DIRECTOR, NATIONAL SECURITY AGENCY

(U) TABLE OF CONTENTS

~~TOP SECRET//SI//ORCON/NOFORN~~

(U) I, George C. Barnes, for my declaration pursuant to 28 U.S.C. § 1746, depose and say as follows:

I. (U) INTRODUCTION

1. **(U)** I am the Deputy Director of the National Security Agency ("NSA"), an intelligence agency within the Department of Defense. I have held this position since May 1, 2017. Prior to serving as Deputy Director, I served as the Director, Workforce Support Activities Directorate, and have been an NSA employee since 1987. I have served in a variety of roles at the Agency, including as NSA's Special United States Liaison Officer in London, where I supported our cryptologic partnership with the United Kingdom and interacted regularly with key U.K. intelligence and cybersecurity leadership, as well as the Chief of Data Acquisition, overseeing NSA's signals intelligence access, collection, and exploitation. I have been designated an original TOP SECRET classification authority under Executive Order No. 13526, 75 Fed. Reg. 707 (Jan. 5, 2010), and Department of Defense Manual No. 5200.1, Vol. 1, Information and Security Program (Feb. 24, 2012).

2. **(U)** The purpose of this declaration is to support an assertion of the military and state secrets privilege (hereinafter, "state secrets privilege") by the Director of National Intelligence ("DNI") in his capacity as head of the Intelligence Community, as well as the DNI's assertion of a statutory privilege under the National Security Act of 1947, *see* 50 U.S.C. § 3024(i)(1), to protect the information described below. The information in question is sought in discovery by the Plaintiff in the above-captioned case, Wikimedia Foundation ("Wikimedia"), and concerns critical NSA intelligence-gathering activities and capabilities. This information is classified, extraordinarily sensitive, and its disclosure reasonably could be expected to cause exceptionally grave damage to the national security of the United States. Through this declaration, I also

hereby invoke and assert the NSA's statutory privilege set forth in Section 6 of the National Security Agency Act of 1959, Public Law No. 86-36 (codified at 50 U.S.C. § 3605(a)), to protect information related to NSA intelligence activities as described herein.

3. **(U)** The statements made herein are based on my personal knowledge of NSA activities and operations, and on information made available to me in my official capacity as the Deputy Director of NSA.

II. (U) CLASSIFICATION OF DECLARATION

4. **(U)**This declaration is classified TOP SECRET//SI//ORCON/NOFORN pursuant to the standards in Executive Order No. 13526. *See* 75 Fed. Reg. 707 (Dec. 29, 2009). Under Executive Order No. 13526, information is classified "TOP SECRET" if unauthorized disclosure of the information reasonably could be expected to cause exceptionally grave damage to the national security of the United States; "SECRET" if unauthorized disclosure of the information reasonably could be expected to cause serious damage to national security; and "CONFIDENTIAL" if unauthorized disclosure of the information reasonably could be expected to cause identifiable damage to national security. At the beginning of each paragraph of this declaration, the letter or letters in parentheses designate(s) the level of classification of the information the paragraph contains. When used for this purpose, the letters "U," "C," "S," and "TS" indicate respectively that the information is either UNCLASSIFIED, or is classified CONFIDENTIAL, SECRET, or TOP SECRET.

5. **(U)** Additionally, this declaration contains Sensitive Compartmented Information (SCI), which is "information that not only is classified for national security reasons as Top Secret, Secret, or Confidential, but also is subject to special access and handling requirements because it involves or derives from particularly sensitive intelligence sources and methods." 28

C.F.R. § 17.18(a). Because of the exceptional sensitivity and vulnerability of such information, these safeguards and access requirements exceed the access standards that are normally required for information of the same classification level. Specifically, this declaration references communications intelligence ("COMINT"), also referred to as special intelligence ("SI"), which is a subcategory of SCI. COMINT or SI identifies SCI that was derived from exploiting cryptographic systems or other protected sources by applying methods or techniques, or from foreign communications.

6. **(U)** Finally, the "ORCON" designator means that the originator of the information controls to whom it is released. In addition to the fact that classified information contained herein and that is contained within the accompanying documents may not be revealed to any person without authorization pursuant to Executive Order 13526, this declaration and many of the accompanying documents contain information that may not be released to foreign governments, foreign nationals, or non-U.S. citizens without permission of the originator and in accordance with DNI policy. This information is labeled "NOFORN."

7. **(U)** Accordingly, none of the information in this declaration can be removed from classified channels without prior classification review by NSA.

III. (U) SUMMARY

8. **(U)** I have been informed that Wikimedia alleges that a technique employed by the NSA to gather foreign intelligence information under Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), known as Upstream surveillance,[1] exceeds the Government's

[1] ~~(TS//SI//NF)~~ [redacted]

authority under FISA, violates the Constitution, and should be permanently enjoined. It is my understanding that the question now before the Court for resolution is whether Wikimedia has legal standing to assert these claims. In an effort to prove its standing, Wikimedia has served a total of 84 discovery requests on the Government, including interrogatories, requests for admission, and document requests. Wikimedia has also taken the deposition of a designated NSA official under Federal Rule of Civil Procedure 30(b)(6). Wikimedia's discovery requests and deposition questions are apparently intended to uncover direct and indirect evidence to support Wikimedia's standing to challenge Upstream surveillance.

9. **(U)** It is my understanding that although the NSA and the other Defendant Government agencies responded to many of Wikimedia's discovery requests, the Government also objected in whole or in part to certain requests based, *inter alia*, on the classified, privileged, and extraordinarily sensitive nature of the national security information Wikimedia sought. The Government also objected to and refused to answer certain deposition questions because they, too, called for classified, privileged, and extraordinarily sensitive national security information. In particular, the Government has objected to any discovery requests or deposition questions that would tend to reveal whether Wikimedia's communications have been subject to Upstream surveillance; operational details of Upstream surveillance; the locations on the Internet backbone where Upstream surveillance is or has been conducted; the types of communications collected through Upstream surveillance; the scope of Upstream surveillance; NSA's cryptanalytic capabilities; and certain additional categories of classified information contained in opinions by, orders from, and submissions to, the Foreign Intelligence Surveillance Court ("FISC") regarding

~~TOP SECRET//SI//ORCON/NOFORN~~

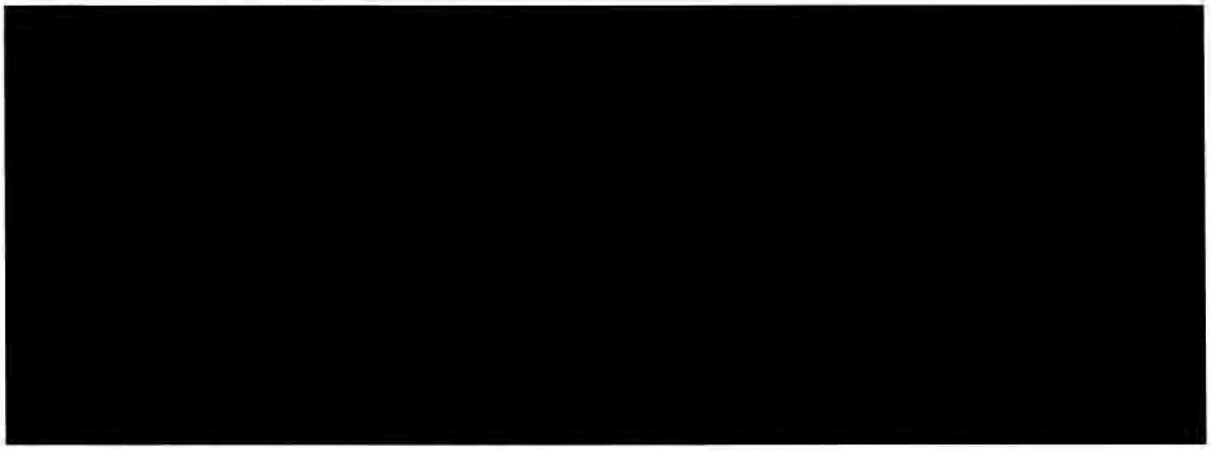
Upstream surveillance. Wikimedia has now moved to compel the disclosure of this classified, privileged, and extraordinarily sensitive national security information.

10. **(U)** This declaration supports the assertion of the state secrets privilege and the statutory privilege under 50 U.S.C. § 3024(i)(1) by the DNI over the classified information that Wikimedia seeks, whether in response to Wikimedia's pending discovery requests, in response to any further discovery requests Wikimedia may serve in this case, or as otherwise may be necessary to litigate Wikimedia's claims or the Government's defenses in this case. I also assert herein the NSA's statutory privilege under 50 U.S.C. § 3605(a) over the same categories of information. As set forth in the accompanying public declaration of the DNI, and explained in classified detail below, the disclosure of the information and documents that Wikimedia seeks could reasonably be expected to cause exceptionally grave damage to the national security of the United States, and therefore must be protected from disclosure and excluded from this case.

11. (~~TS//SI//NF~~) [redacted]

[redacted]

[2] (~~TS//SI//NF~~) [redacted]



12. **(U)** The facts at issue include, first, whether or not any of Wikimedia's communications, or of other individuals and entities, have been subject to Upstream surveillance. As a matter of course, the Government cannot publicly confirm or deny whether any individual or organization is or has been subject to NSA intelligence-gathering activities, because to do so would tend to reveal to our adversaries who are the NSA's actual targets of surveillance and who are not, which channels of communication are free from NSA surveillance and which are not, and other sensitive intelligence methods and sources, thereby helping our adversaries evade detection and capitalize on limitations in the NSA's surveillance capabilities.

13. **(U)** As further explained below, it is also essential to protect information concerning the operational details of Upstream surveillance, as well as the location(s) on the Internet "backbone" where Upstream surveillance is conducted; the types of communications collected through Upstream surveillance; the scale and scope of Upstream surveillance; NSA's cryptanalytic capabilities; and additional categories of classified information contained in opinions, orders, and submissions to the FISC concerning Upstream surveillance that Wikimedia seeks in discovery. Notwithstanding the Government's disclosure of certain facts, in order to promote transparency and public understanding about the Upstream program, the additional

disclosure of the information Wikimedia seeks to compel could reasonably be expected to cause exceptionally grave damage to national security.

14. **(U)** Most obviously, the disclosure of the information Wikimedia seeks would reveal to foreign adversaries the NSA's operational methods and capabilities (or lack thereof), and specific channels of communication from which the NSA has in the past and continues today to obtain intelligence information, thus enabling them to evade particular channels that are being monitored, to exploit channels that are not subject to NSA collection, to target for hostile action the facilities where the NSA obtains critical foreign intelligence, and to exploit the NSA's sources and methods of surveillance for their own purposes. In addition, the information that Wikimedia seeks would also tend to reveal the identities of specific foreign targets of foreign intelligence surveillance that NSA conducts pursuant to Section 702, alerting them that their activities have been detected by the U.S. Intelligence Community. In all cases, these disclosures would risk exceptionally grave damage to national security.

15. **(U)** For all of these reasons and others explained below, I support the DNI's assertion of the state secrets privilege and the statutory privilege under 50 U.S.C. § 3024(i)(1) to prevent the disclosure of information falling within the categories described herein. I also assert the NSA's statutory privilege under Section 6 of the National Security Agency Act, 50 U.S.C. § 3605(a), over the same information, which concerns NSA intelligence functions. The information Wikimedia seeks must be protected from disclosure and excluded from this case to avoid risking exceptionally grave damage to the national security of the United States

IV. (U) BACKGROUND

A. (U) The National Security Agency and Its Signals Intelligence Mission

16. **(U)** The NSA was established by Presidential Directive in 1952 as a separately organized agency within the Department of Defense. The NSA's foreign intelligence mission includes the responsibility to collect, process, analyze, produce, and disseminate signals intelligence ("SIGINT") information, of which COMINT is a significant subset, for (a) national foreign intelligence purposes, (b) counterintelligence purposes, and (c) the support of military operations. *See* Executive Order 12333, § 1.7(c), as amended.[3]

17. **(U)** SIGINT consists of three subcategories: (1) COMINT; (2) electronic intelligence ("ELINT"); and (3) foreign instrumentation signals intelligence ("FISINT"). COMINT is defined as "all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients." 18 U.S.C. § 798. COMINT includes information derived from the interception of foreign and international communications, such as voice, facsimile, and computer-to-computer information conveyed via a number of means (*e.g.*, microwave, satellite links, high frequency/very high frequency ("HF/VHF") broadcast). ELINT is technical intelligence information derived from foreign non-communications electromagnetic radiations except atomic detonation or radioactive sources—in essence, radar systems affiliated with military weapons platforms (*e.g.*, anti-ship) and civilian systems (*e.g.*, shipboard and air traffic control radars). FISINT is derived from the

[3] **(U)** Executive Order 12333, reprinted as amended in 50 U.S.C § 3001 note, generally describes the NSA's authority to collect foreign intelligence not subject to FISA's definition of electronic surveillance, including activities undertaken abroad. Section 1.7(c) of E.O. 12333, as amended, specifically authorizes the NSA to "[c]ollect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information for foreign-intelligence and counterintelligence purposes to support national and departmental missions."

intercept of foreign electromagnetic emissions associated with the testing and operational deployment of non-U.S. aerospace, surface, and subsurface systems.

18. **(U)** The NSA's SIGINT responsibilities include establishing and operating an effective unified organization to conduct SIGINT activities set forth in E.O. 12333, § 1.7(c)(2), as amended, and 50 U.S.C. § 3038(b)(1). In performing its SIGINT mission, the NSA has developed a sophisticated worldwide SIGINT collection network that acquires, among other things, foreign and international electronic communications and related information. The technological infrastructure that supports the NSA's foreign intelligence information collection network has taken years to develop at a cost of billions of dollars and untold human effort. It relies on sophisticated electronic data collection and processing technology.

19. **(U)** There are two primary reasons for gathering and analyzing foreign intelligence information. The first, and most important, is to gain information required to direct U.S. resources as necessary to counter external threats and in support of military operations. The second reason is to obtain information necessary to the formulation and promotion of U.S. foreign policy. Foreign intelligence information provided by the NSA is thus relevant to a wide range of important issues, including military order of battle; threat warnings and readiness; cybersecurity; arms proliferation; international terrorism; counterintelligence; and foreign aspects of international narcotics trafficking.

20. **(U)** The NSA's ability to produce foreign intelligence information depends on its access to foreign and international electronic communications. Foreign intelligence produced by COMINT activities, of which NSA's acquisition of foreign communications pursuant to FISA (to include Upstream 702 collection) is a subset, is an extremely important part of the overall foreign intelligence information available to the United States and is often unobtainable by other

means. Public disclosure of either the capability to collect specific communications or the substance of the information derived from such collection itself can easily alert targets to the vulnerability of their communications. Disclosure of even a single communication holds the potential of revealing intelligence collection techniques that are applied against targets around the world. Once alerted, targets can frustrate COMINT collection by using different or new encryption techniques, by disseminating disinformation, or by utilizing a different communications link. Such evasion techniques may inhibit access to the target's communications and therefore deny the United States access to information crucial to the defense of the United States both at home and abroad. COMINT is provided special statutory protection under 18 U.S.C. § 798, which makes it a crime to knowingly disclose to an unauthorized person classified information "concerning the communication intelligence activities of the United States or any foreign government." Disclosure of the NSA's Upstream collection techniques would also negatively impact the Agency's ability to execute COMINT activities pursuant to E.O. 12333, given the overlap in the technical and operational details of both sets of collection activities.

B. (U) External Threats to the National Security of the United States

21. **(U)** The threat of international terrorism originally gave rise to the NSA intelligence activities challenged in this lawsuit. As a result of the unprecedented attacks of September 11, 2001, the United States found itself immediately propelled into a conflict with al Qaeda and its associated forces, and later their successors, groups that still possess the evolving capability and intention of inflicting further attacks on the United States.

22. **(~~S//NF~~)** [redacted]

[redacted]

~~TOP SECRET//SI//ORCON/NOFORN~~

[redacted]

23. (~~TS//SI//NF~~) [redacted]

[redacted]

24. (~~TS//SI//NF~~) [redacted]

[redacted]

[redacted]

25. **(U)** Protecting U.S. national security against our foreign adversaries therefore presents critical challenges for the Nation's communications intelligence capabilities. One advantage enjoyed by the NSA in meeting these challenges stems from the fact that the United States long has been and remains a critical hub for the transmission and routing of electronic

[4] **(~~S//NF~~)** [redacted]

communications traveling on the global telecommunications network. Because of the United States' position as a global communications hub, hostile foreign actors often communicate using providers or services based in the United States, but, even when the NSA's foreign intelligence targets use foreign-based providers or services, their communications are often routed through the United States regardless of their country of origin or their ultimate destination. NSA SIGINT activities in the United States seek to exploit this "home field" advantage to discover and intercept our adversaries' communications in order to provide the timely, insightful, and precise intelligence needed to take decisive action against these external threats to our security.

26. (~~S//NF~~) [redacted]

[redacted]

C. (U) Collection of Communications Content Pursuant to FISA Section 702

27. **(U)** In July 2008, Congress enacted the Foreign Intelligence Surveillance Act Amendments Act of 2008 (the "FAA"), Pub. L. 110-261, 122 Stat. 2436. The FAA added a new section 702 to FISA, 50 U.S.C. § 1881a ("Section 702"), which created new statutory authority permitting the targeting of non-United States persons reasonably believed to be outside of the United States to acquire foreign intelligence information without individualized orders or warrants from the FISC. More specifically, Section 702 generally provides that, upon the FISC's

approval of a "certification" submitted by the Government, the Attorney General and the DNI may jointly authorize, for up to one year, the "targeting of [non-U.S.] persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. § 1881a(a), (h).[5] Although the statute does not require the government to identify the specific facilities, places, premises, or property at which an authorized acquisition will be directed, the government must certify that an acquisition involves obtaining foreign intelligence information "from or with the assistance of an electronic communication service provider." *Id.* § 1881a(h)(2)(A)(vi).

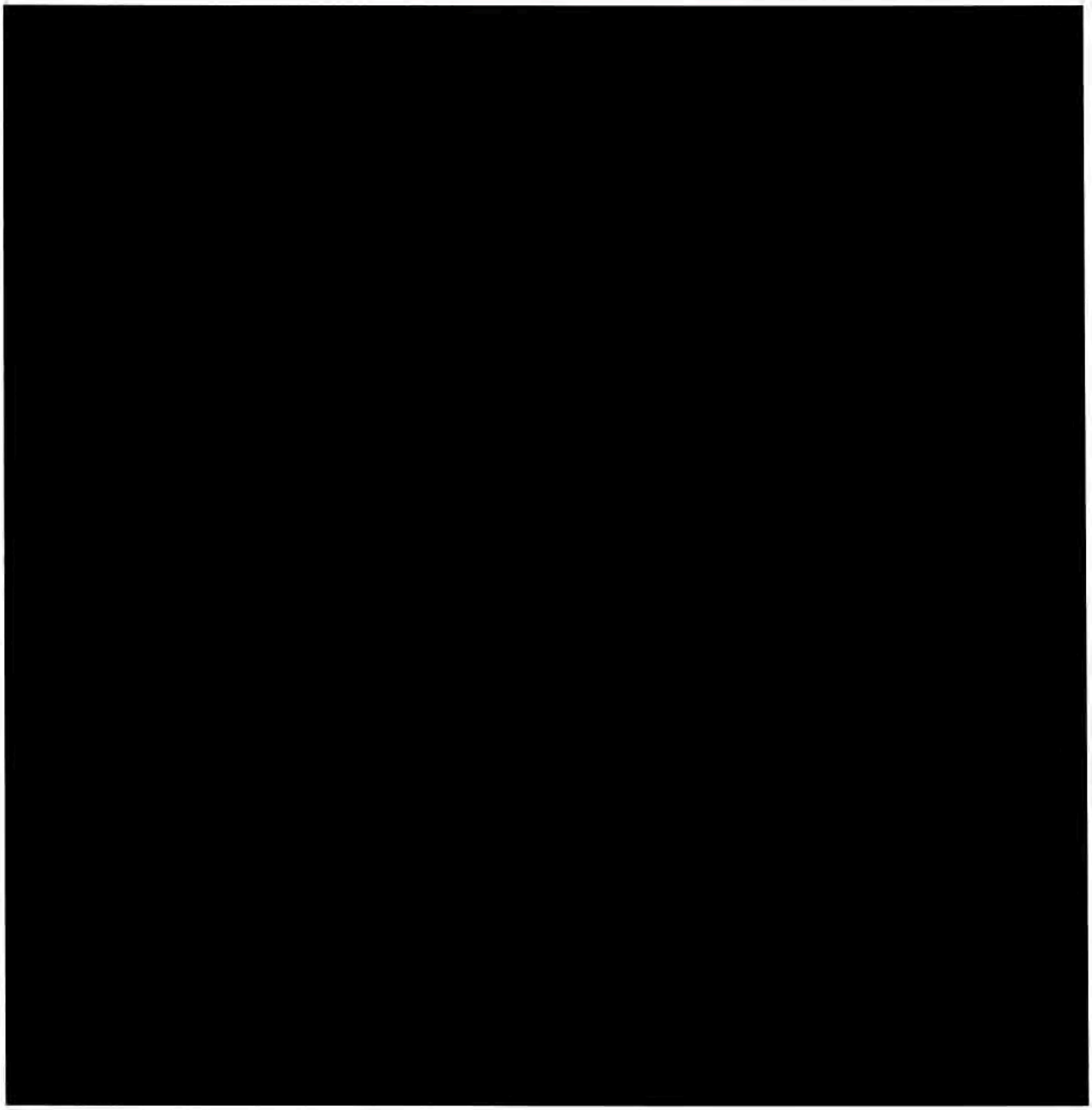
28. **(U)** Accordingly, under Section 702, the Attorney General and the DNI submit annual certifications to the FISC for its approval, as required under the statute, to authorize the targeting of non-U.S. persons reasonably believed to be located outside of the United States to acquire foreign intelligence information. These certifications identify categories of foreign intelligence information authorized for acquisition, but do not identify the particular non-U.S. persons who will be targeted. Instead, the certifications include targeting procedures, approved

[5] **(U)** Section 702 has always imposed four requirements that must be met for FISC approval of a Section 702 certification. First, the Attorney General and the DNI must certify, *inter alia*, that a significant purpose of the acquisitions is to obtain foreign-intelligence information, as that term is defined under FISA, and the FISC must find that the Attorney General and DNI's certification contains all of the required statutory elements. 50 U.S.C. § 1881a(h)(2)(A)(iv), (j)(2)(A). Second, the FISC must find that the Government's targeting procedures are reasonably designed to ensure that acquisitions conducted under the authorization are limited to targeting non-U.S. persons reasonably believed to be located outside the United States, and will not intentionally acquire communications known at the time of acquisition to be purely domestic. *Id.* § 1881a(j)(2)(B). Third, the FISC must find that the Government's minimization procedures meet FISA's requirements. *Id.* §§ 1801(h), 1821(4), 1881a(j)(2)(C). And fourth, the FISC must find that the Government's targeting and minimization procedures are consistent, not only with FISA, but also with the requirements of the Fourth Amendment. *Id.* § 1881a(i)(3)(A). Following passage of the FISA Amendments Reauthorization Act of 2017 earlier this year, the FISC must now also find that the Government's querying procedures meet the statutory requirements and are consistent with the Fourth Amendment. *Id.* § 1881a(j)(2)(D); (j)(3)(A).

by the Attorney General, which must, among other things, be reasonably designed to ensure that any Section 702 acquisition is limited to targeting persons reasonably believed to be located outside the United States, and to prevent the intentional acquisition of wholly domestic communications. In addition, the targeting procedures specify the manner in which the Intelligence Community determines whether a person is a non-U.S. person reasonably believed to be located outside the United States who is likely to possess, receive, or communicate foreign intelligence information authorized for acquisition by a certification.

29. ~~(S//NF)~~ [redacted]

30. ~~(TS//SI//NF)~~ [redacted]



[6] **(U)** Generally speaking, the Internet "backbone" refers to the interconnected networks of providers' long-haul terrestrial, fiber-optic cables that carry large volumes of Internet communications over long distances, usually between large metropolitan areas, and interchange communications traffic around the world. The Internet backbone also includes the high-capacity submarine telecommunications cables that carry Internet communications between different parts of the globe.

31. (~~S//NF~~) [redacted]

[redacted]

D. (U) Upstream Collection

32. (~~S//NF~~) [redacted]

[redacted]

33. **(U)** Over the past several years, the Government has declassified and publicly released thousands of pages of materials pertaining to Section 702 collection activities, including

Upstream surveillance, such as redacted memorandum opinions and orders issued by the FISC and certain of NSA's Section 702 targeting and minimization procedures. In addition, two Government reports have been issued that address Section 702 activities, including Upstream surveillance. In April 2014, the NSA's Civil Liberties and Privacy Office released a report on the NSA's implementation of FISA Section 702, which included a high-level unclassified description of Upstream. A short time later, in July 2014, the Privacy and Civil Liberties Oversight Board ("PCLOB"), an independent Executive Branch agency established pursuant to statute, 42 U.S.C. section 2000ee, issued its report on the Government's implementation of Section 702, which also included an unclassified description of the Upstream program. *See* PCLOB, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("PCLOB Section 702 Report").

34. **(U)** While these declassified documents and unclassified reports describe the Upstream acquisition process in general terms, they are necessarily incomplete because certain operational details of Upstream acquisition remain highly classified.

35. **(~~TS//SI//NF~~)** [redacted]

[redacted]

[7] **(~~TS//SI//NF~~)** [redacted]

[redacted]

[redacted]

36. (~~TS//SI//NF~~) [redacted]

[redacted]

[8] (~~TS//SI//NF~~) [redacted]

[9] (~~TS//SI//NF~~) [redacted]

[redacted]

37. (~~TS//SI//NF~~) [redacted]

[redacted]

38. (~~TS//SI//NF~~) [redacted]

[redacted]

[10] **(U)** IP addresses identify devices on the Internet or other computer networks, and are used to route packets between destinations on a computer network. Public IP addresses are allocated to organizations (*e.g.*, companies, governments, universities, etc.), who register the basic ownership details (to include country) with a regional registry. The organizations that are allocated IP addresses may have network devices outside of the country listed in regional registry entry, thereby enabling IP addresses to be associated with network devices outside of the registered country. IP filtering refers to blocking or selecting communications to or from particular groups of IP addresses (which may include single IP addresses).

[redacted]

39. (~~TS//SI//NF~~) [redacted]

[redacted]

40. (~~TS//SI//NF~~) [redacted]

[redacted]

[redacted]

41. **(U)** It is against this backdrop that the risks of disclosing the information that Wikimedia seeks to compel the Government to reveal should be assessed.

E. (U) The Wikimedia Discovery Requests

42. **(U)** As discussed above, Wikimedia, seeking evidence with which to establish its legal standing to bring a legal challenge to Upstream surveillance, served 84 separate discovery requests on the Government. I am advised that Wikimedia has moved to compel further responses by the Government to 53 of those requests, and that it divides them into three categories.

43. **(U)** The first category Wikimedia describes as "direct evidence" that it "has been surveilled" in the course of Upstream surveillance, i.e., that at least some of its communications have been copied, scanned, retained, or otherwise "interacted with" by the NSA. The Government has refused to confirm or deny, however, whether the NSA has copied, scanned, retained, or otherwise "interacted with" Wikimedia communications in the course of Upstream surveillance (see Wikimedia Requests for Admission ("RFA") Nos. 34-36); has refused to confirm or deny the authenticity of purported Power Point slides that, according to Wikimedia, express NSA interest in surveilling its communications (RFA Nos. 16-21); and has refused to confirm or deny whether the NSA possesses any communications of Wikimedia's acquired in the course of Upstream surveillance, or any other documents concerning interactions with Wikimedia communications during the Upstream collection process (Wikimedia Requests for Production ("RFP") Nos. 23-24). Disclosure of this information reasonably can be expected to cause exceptionally grave damage to the national security of the United States.

44. **(U)** The second category of information that Wikimedia seeks in its motion to compel is described therein as "[k]ey terms used in describing Upstream surveillance to the public." This category includes information responsive to interrogatories asking the Government to describe its understanding of the "definitions" of a list of terms and phrases used in unclassified public documents to discuss various aspects of Upstream surveillance. *See* Wikimedia Interrogatory Nos. 1-9. In response the Government set forth its understanding of most of these terms and phrases, so far as it could do so without revealing classified information regarding the sources and methods and technical operational details of Upstream surveillance.

45. **(U)** The Government was unable to provide any unclassified response, however, to Wikimedia's Interrogatory Nos. 1 and 7. Interrogatory No. 1 sought the Government's understanding of the term "international Internet link," as used by the FISC in an October 3, 2011, memorandum opinion concerning Upstream surveillance. "International Internet link" is not a term commonly used in the telecommunications industry. The Government has its own understanding of what the FISC meant when the FISC used that term, but, because that understanding is based on still-classified portions of the FISC's October 3, 2011, opinion, the Government cannot explain its understanding of what the FISC meant by the term "international Internet link" without revealing classified information.

46. **(U)** Interrogatory No. 7 asks the Government to state its understanding of the common features of Internet packets that comprise an "Internet transaction." "Internet transaction" is also not a term commonly used in the telecommunications industry, but a term defined in the NSA's Section 702 Minimization Procedures to help explain that the NSA's Upstream collection devices do not necessarily acquire just single communications but packets of communications data that may form either a single, discrete communication, or multiple

communications. The Government, however, was unable to state the common features of the packets of data constituting an Internet transaction, as Wikimedia requested, without revealing, or tending to reveal, classified information about the design and operation of the NSA's Upstream surveillance equipment.

47. **(U)** Wikimedia also includes in its second category of discovery RFP Nos. 21 and 22, which ask the Government to produce all FISC, Foreign Intelligence Surveillance Court of Review, and Supreme Court opinions and orders concerning Upstream surveillance, and all submissions to these courts concerning Upstream surveillance,[11] since the enactment of Section 702 in July 2008, regardless of whether they include any of the information otherwise sought by the requests in this category. The Government objected to producing these documents on the grounds that, among other reasons, their disclosure could reasonably be expected to cause exceptionally grave damage to the national security of the United States. In addition, I am told that the volume of documents called for by RFP Nos. 21 and 22 exceeds 10,000 pages, and thus the Government also objected to the burden of producing unclassified versions of such a large body of classified materials.

48. **(U)** The third and largest category of discovery requests to which Wikimedia seeks to compel responses is labeled in Wikimedia's motion to compel as "Evidence concerning the scope and breadth of Upstream surveillance." The requests in this wide-ranging category ask the Government (i) to state the percentage of international Internet circuits and submarine cables that were "monitored" in the course of Upstream surveillance during each of the years 2015-2017 (Interrogatory Nos. 16-17); (ii) to admit whether the NSA conducts Upstream surveillance

[11] **(U)** The Government has not made submissions to the FISC-R or the Supreme Court specifically concerning Upstream collection and nor has either Court issued an opinion or order specifically concerning Upstream collection.

on multiple Internet backbone circuits, chokepoints, and international Internet links (RFA Nos. 13-15); (iii) to admit the authenticity of documents that, according to Wikimedia, indicate locations on the Internet backbone where the NSA conducts Upstream surveillance (RFA Nos. 25-30, 39); (iv) to state the amount of Internet communications traffic that was "filtered" and "scanned" in the course of Upstream surveillance during each of the years 2015-2017 (Interrogatory Nos. 18-19); (v) to admit whether the contents of Internet web traffic (HTTP and HTTPS communications) are now and previously were scanned in the course of Upstream surveillance (RFA Nos. 37-38); (vi) to admit whether the NSA, in conducting Upstream surveillance, copies, and reviews in bulk the contents of Internet communications that are in transit and neither to nor from Upstream surveillance targets (RFA Nos. 6-10); (vii) to describe the entire process by which the contents of Internet communications are in any way "interacted with" during the Upstream process, including any inaccuracies in the description provided in the PCLOB Section 702 Report (Interrogatory Nos. 14-15); and (viii) to identify the protocols used to encrypt Internet communications that the NSA is capable of decrypting (Interrogatory No. 20; RFA No. 40).

49. **(U)** Wikimedia also includes in this third category eight separate requests for the production of documents, seeking (i) documents sufficient to show the total number of circuits on which Upstream surveillance was conducted, the total bandwidth of those circuits, and the total number of Internet transactions acquired, during each of the years 2010-2017 (RFP Nos. 10, 13, 14); (ii) documents sufficient to show the number of "international Internet links" that were "monitored" in the course of Upstream surveillance during each of the years 2015-2017 (RFP No. 15); (iii) documents sufficient to show the number of international Internet "chokepoints" at which the NSA has allegedly conducted Upstream surveillance at any time since Section 702

was enacted in July 2008 (RFA No. 16); and (iv) the targeting procedures applied for purposes of implementing Upstream surveillance in the years 2009, 2015, and 2017 (RFP No. 18). In addition, Wikimedia includes in this "scope and breadth" category RFP Nos. 21 and 22, which call for the production of more than 10,000 pages of classified orders and opinions issued by and submissions made to the FISC, regardless of whether they contain any of the information otherwise sought in category three.

50. **(U)** The Government was able to provide partial, unclassified responses to Wikimedia's RFA Nos. 6, 8, and 10 (concerning the review of communications during the Upstream collection process), and partial responses to several of the document requests in this category. But because of the highly classified and extraordinarily sensitive nature of the documents and information sought in Wikimedia's third category of discovery requests, it was otherwise necessary for the Government to object to producing the documents and information sought in this category in order to protect classified information whose disclosure could reasonably be expected to cause exceptionally grave damage to national security.

51. **(U)** In addition to the foregoing three categories of discovery requests, Wikimedia also seeks to compel further testimony from an NSA official who was deposed on April 16, 2018, who had been designated to testify on behalf of the NSA on the following topics: (i) the definitions and meaning, as understood by the NSA, of terms that have been used in official public disclosures to describe Upstream surveillance; (ii) the ways in which the NSA (or telecommunications service providers acting on the NSA's behalf) access or interact with Internet communications in the course of Upstream surveillance; (iii) the number and type of Internet communications or transactions intercepted, accessed, copied, filtered, reviewed, screened, scanned, ingested, and/or retained by the NSA in the course of Upstream surveillance;

(iv) the number of circuits, international Internet links, and Internet backbone checkpoints on or at which the NSA conducts and has conducted Upstream surveillance; and (v) the facts related to Upstream surveillance that the NSA has disclosed, or authorized disclosure of, to the FISC, the Foreign Intelligence Surveillance Court of Review, the Supreme Court, and/or the PCLOB, and that it has subsequently declassified.

52. **(U)** The designated deponent, Rebecca J. Richards, has served as the Director of Civil Liberties and Privacy at NSA since February 2014. As NSA's Chief Transparency Officer, Ms. Richards works to communicate with the public about the value of signals intelligence and the tools NSA needs to conduct its mission, while maintaining protection over NSA's vital sources and methods. These duties and responsibilities require that she maintain a high level of familiarity with the operational details of a wide range of NSA intelligence activities, including Upstream surveillance. I have been advised that Ms. Richards was questioned for approximately seven hours on the record on topics concerning Upstream surveillance that were largely coextensive with the subjects covered by Wikimedia's written discovery requests. I understand that because the questions posed by Wikimedia's counsel consistently called for classified details about the sources, methods and operational details of Upstream surveillance, it was necessary throughout the deposition for the Government to object to Wikimedia's questions, and to withhold information, in whole or in part, in response thereto, in order to protect classified information whose disclosure could reasonably be expected to cause exceptionally grave damage to the national security of the United States.

V. (U) INFORMATION SUBJECT TO ASSERTIONS OF PRIVILEGE

53. **(U)** As discussed above, the Government has officially declassified and publicly disclosed certain information about the existence and nature of NSA Upstream surveillance.

However, the additional information that Wikimedia seeks to compel the Government to disclose in response to its discovery requests and certain deposition questions remains properly classified, and is subject to the DNI's assertions of the state secrets privilege, to the DNI's assertion of the statutory privilege under 50 U.S.C. § 3024(i)(1), and to my own assertion herein of the NSA's statutory privilege under 50 U.S.C. § 3605(a). Although, as discussed above, I have been advised that Wikimedia divides the classified information it seeks into the three categories discussed above, for purposes of understanding the exceptionally grave risks to national security that would flow from disclosing this information, the information sought is best understood as falling into the seven separate categories identified below. For the Court's ease of reference, I note below each of Wikimedia's written discovery requests that calls for, or implicates, classified information in each category. I have been informed that the classified information that Wikimedia sought to elicit during Ms. Richards's deposition falls into all seven categories. The information encompassed by these categories would remain classified, and privileged, regardless of whether it is sought in response to pending or future discovery requests served by Wikimedia, or may become necessary for any other purposes associated with the litigation of Wikimedia's claims or the Government's defenses in this case.

54. **(U)** Accordingly, in general and unclassified terms, the DNI's assertion of the state secrets privilege, of the statutory privilege under 50 U.S.C. § 3024(i)(1), and my assertion of the NSA's statutory privilege under 50 U.S.C. § 3605(a), encompass the following categories of still-classified information and properly protected national security information concerning NSA Upstream surveillance:

A. **(U) Entities subject to Upstream surveillance activities:** Documents and information responsive to Wikimedia's pending discovery requests, to any future discovery that Wikimedia may seek, or that may otherwise be necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this litigation, that indicate or may tend to indicate whether communications of Wikimedia, and/or of other individuals and entities, have been subject to Upstream surveillance activities [RFA Nos. 16-21, 34-36; RFP Nos. 21-24];

B. **(U) Operational details of the Upstream collection process:** Documents and information responsive to Wikimedia's pending discovery requests, to any future discovery that Wikimedia may seek, or that may otherwise be necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this litigation, that reveal or may tend to reveal still classified technical details concerning the methods, processes, and devices employed (including the design, operation, and capabilities of the devices employed) to conduct Upstream surveillance [Interrogatory Nos. 3-5, 14, 15; RFA Nos. 6-10, 37, 38; RFP Nos. 21, 22];

C. **(U) Locations at which Upstream surveillance is conducted:** Documents and information responsive to Wikimedia's pending discovery requests, to any future discovery that Wikimedia may seek, or that may otherwise be necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this litigation, that reveal or may tend to reveal still classified information about any specific location(s), or the nature of the location(s), on the Internet backbone network(s) of U.S. electronic communication service provider(s) at which Upstream surveillance is conducted [Interrogatory Nos. 1, 2; RFA Nos. 13-15, 25-30, 39; RFP Nos. 13, 15, 16, 18, 21, 22];

D. **(U) Categories of Internet-based communications subject to Upstream surveillance activities:** Documents and information responsive to Wikimedia's pending discovery requests, to any future discovery that Wikimedia may seek, or that may otherwise be necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this litigation, that reveal or may tend to reveal still classified information about the specific types or categories of communications either subject to or acquired in the course of the Upstream collection process [Interrogatory Nos. 6-8; RFA Nos. 16-18; RFP No. 22];

E. **(U) The scope and scale on which Upstream surveillance is or has been conducted:** Documents and information responsive to Wikimedia's pending discovery requests, to any future discovery that Wikimedia may seek, or that may otherwise be necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this litigation, that reveal or may tend to reveal still classified information about (i) the volume or proportion of Internet communications traffic, including international Internet communications, either subject to or acquired in the course of the Upstream collection process, (ii) the number, proportion, and/or bandwidth of any circuit, international submarine or terrestrial cable, or other Internet backbone link, on which Upstream surveillance

is or has been conducted; and (iii) any other measure of the scope or scale on which Upstream surveillance is or has been conducted [Interrogatory Nos. 9, 16-19; RFP Nos. 10, 14];

F. **(U) NSA's cryptanalytic capabilities:** Documents and information responsive to Wikimedia's pending discovery requests, to any future discovery that Wikimedia may seek, or that may otherwise be necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this litigation, that reveal or may tend to reveal still classified information about the NSA's capability, or lack thereof, to decrypt, circumvent, or defeat specific types of communications security protocols [Interrogatory No. 20; RFA No. 40]; and

G. **(U) Additional categories of classified information contained in opinions and orders issued by, and in submissions made to, the FISC:** The additional categories of classified information contained in the documents responsive to Wikimedia RFP Nos. 21 and 22, not already encompassed by categories A-F, above, as set forth in the privilege log served by Defendant U.S. Department of Justice on March 19, 2018 [RFP Nos. 21, 22]

VI. (U) HARM OF DISCLOSURE OF PRIVILEGED INFORMATION

A. (U) Information Concerning Whether Communications of Wikimedia or of Other Entities or Individuals Have Been Subjected to Upstream Surveillance Activities [RFA Nos. 16-21, 34-36; RFP Nos. 21-24]

55. **(U)** The first category of information as to which I am supporting the DNI's assertions of privilege, and asserting the NSA's statutory privilege, concerns documents and information that would reveal or tend to reveal whether communications of Wikimedia or of other entities or individuals have been subject to any stage of the Upstream collection process.

56. **(U)** As discussed above, Wikimedia seeks to compel the Government to admit or deny whether the NSA has copied, reviewed the content of, and/or retained at least one Wikimedia communication in the course of Upstream surveillance; to produce any Wikimedia communications the NSA has copied, reviewed, or otherwise interacted with; and to produce any documents concerning such NSA "interaction" with Wikimedia communications. See RFA Nos. 34-36, RFP Nos. 23-24. In addition, Wikimedia seeks to compel the Government to confirm or deny the authenticity of purportedly classified documents indicating, according to Wikimedia,

that the NSA targets its communications for Upstream surveillance. RFA Nos. 16-21. These matters were also the subjects of questions propounded by Wikimedia to the NSA's designated deposition witness, who was instructed for reasons of privilege that she should not answer. Documents responsive to Wikimedia RFP Nos. 21 and 22, regarding court orders, opinions, and submissions concerning Upstream surveillance, also include information about the nature or specific identities of individual Upstream surveillance targets, and of entities about which the NSA seeks to acquire intelligence information. See, e.g., Department of Justice Privilege Log dated March 19, 2018 ("DOJ Privilege Log") at Nos. 18, 23, 29, 31. For the reasons set forth below, disclosure of such information by the NSA reasonably could be expected to cause exceptionally grave damage to national security, because it would reveal information as to whether particular entities have been subject to surveillance, as well as the nature, scope, and extent of NSA Upstream surveillance activities.

57. **(U)** As a matter of course, the NSA cannot publicly confirm or deny whether particular individuals or entities are or have been subject to intelligence-gathering activities, because to do so would tend to reveal actual targets or subjects. The harm of revealing the identities of persons or organizations who are the actual targets or subjects of foreign-intelligence gathering is relatively straightforward. If individuals or organizations knew or suspected they are targets of subjects of U.S. intelligence activities, they would naturally tend to alter their behavior to take new precautions against such scrutiny. In addition, revealing which individuals or entities are not targets or subjects of intelligence gathering would indicate who has avoided surveillance or collection, and which channels of communication may be secure. Such information could allow actual or potential adversaries, secure in the knowledge that they are not under government scrutiny, to convey information necessary or useful to the execution of hostile

acts against the United States and its interests. Alternatively, such individuals or entities may be unwittingly utilized or even forced by foreign adversaries to convey information through secure channels. Revealing which channels are free from surveillance and which are not could also reveal sensitive intelligence methods, and thereby help an adversary evade detection and capitalize on limitations in the NSA's surveillance capabilities.

58. **(U)** Similar harms would result from confirming or denying whether the communications of particular persons or entities have been subject to collection, even where it may be assumed that they are law-abiding and not likely to be actual targets or subjects of such activity. This is so because, if the NSA were to confirm that specific individuals or entities have not been targets of or subject to collection (*i.e.*, that their communications have not been intercepted), but later refuse to comment (as it would have to) in situations involving actual targets or subjects, actual or potential adversaries of the United States could then easily deduce that the persons in the latter instances are or have been targets of or subject to surveillance. In addition, disclosing whether communications of particular persons or organizations have or have not been targeted, or intercepted through the targeting of third parties, would reveal whether particular channels of communication are secure, and also reveal to third-party targets whether their own communications may be secure. Moreover, each occasion where the Government confirms (even if compelled to confirm) that certain persons or organizations have or have not been subjects of surveillance makes it more difficult in the future to withhold information about the surveillance status of other individuals or entities. This could result in a cascading effect of disclosures.

59. **(U)** To appreciate the national security risks associated with disclosing whether the NSA, through Upstream surveillance, has copied, reviewed, retained, or otherwise interacted

with Wikimedia's communications, it is necessary to understand that Wikimedia has placed three types of its communications at issue in this case: (i) online communications between Wikimedia websites and individuals who read, contribute to, or edit the contents of those websites, using the HTTPS and HTTP protocols; (ii) Wikimedia's internal "logs" of such communications with its websites, whose logs are transmitted from its servers in Amsterdam to its servers in the United States; and (iii) electronic communications of Wikimedia's U.S. staff with Wikimedia staff, contractors, and volunteers located in other countries. Disclosing (be it through admission, or the production of documents) whether Wikimedia communications have been subject to copying, reviewing, or any other alleged form of "interaction" in the Upstream collection process, would entail confirmation of whether Wikimedia's HTTPS/HTTP communications, its "log" communications, and/or its staff communications have been subjected to Upstream surveillance.

60. (~~TS//SI//NF~~) [redacted]

[redacted]

[redacted]

61. (~~TS//SI//NF~~) [redacted]

62. **(U)** Revealing whether the NSA, in the course of Upstream surveillance, has collected or otherwise interacted with the online communications of Wikimedia's U.S. staff, or the personnel of any organization that communicates routinely over the Internet, could reveal to targeted individuals or entities in communication with that organization that they may be subject to NSA surveillance. That is especially the case were the Government actually to produce any communications with the subject organization that it has acquired, as has been demanded here. The presence or absence, among the disclosed communications, of exchanges with targets that

had been in contact with the subject organization could alert them to surveillance of which they had been unaware, or provide assurance that their communications are secure. In either event, national security could be imperiled. The presence or absence of communications to or from particular countries could also alert other potential targets within those countries to whether NSA seeks to collect communications to or from that country.

63. **(U)** In search of "direct evidence" that its communications have been subject to Upstream surveillance, Wikimedia also demands that the Government confirm or deny whether two purportedly classified Power Point slides (reproduced on page four of its motion to compel) are in fact genuine NSA documents indicating that the NSA targets Wikimedia communications (and HTTP communications generally) for Upstream surveillance. For the reasons just discussed, including the dangers of alerting our adversaries to the types of communications on which the NSA does or does not focus its surveillance efforts, the Government cannot confirm or deny the authenticity of the so-called "NSA slides" without damaging national security.

64. **(U)** Specifically, RFA Nos. 16-18 refer to a slide, entitled: "Why are we interested in HTTP?" while RFA Nos. 19-21 relate to a slide, entitled: "Fingerprints and Appids." Wikimedia requests the Government to admit that both documents are "genuine" NSA documents containing statements by NSA "employees on matters within the scope of their employment during the course of their employment," and that these NSA employees were "authorized to make statements on the subjects of the statements within the document."

65. **(~~TS//SI//NF~~)** [redacted]

[redacted]

66. (~~TS//SI//NF~~) [redacted]

[redacted]

67. (~~TS//SI//NF~~) [redacted]

[redacted]

68. (~~TS//SI//NF~~) [redacted]

[redacted]

[redacted]

69. (~~TS//SI//NF~~) [redacted]

70. **(U)** Finally, as reflected in the DOJ Privilege Log, a substantial number of the classified orders, opinions, and court submissions concerning Upstream surveillance that are responsive to Wikimedia's RFP Nos. 21 and 22 contain information about the nature or specific identities of individual Upstream surveillance targets, and of entities about which the NSA seeks to acquire intelligence information under Section 702. For the reasons discussed herein, the Government cannot disclose such information about the nature and identities of the NSA's actual surveillance targets without risking exceptionally grave damage to national security.

71. **(U)** For all of the above-noted reasons, disclosing information tending to confirm or deny whether communications of Wikimedia, or of other entities or individuals, have been subject to any stage of the Upstream collection process could reasonably be expected to cause exceptionally grave damage to the national security of the United States.

B. (U) Operational Details of the Upstream Collection Process
[Interrogatory Nos. 3-5, 14-15; RFA Nos. 6-10, 37, 38; RFP Nos. 21, 22]

72. (~~S//NF~~) [redacted]

[redacted]

73. **(U)** As discussed above, the Government has officially acknowledged the existence of Upstream surveillance and has publicly released a limited amount of information describing, at a high level of generality, how Upstream collection operates. The Government has produced this now-unclassified information about Upstream's operation in response to Wikimedia's discovery requests. Wikimedia now seeks additional technical details about the Upstream collection process, information that remains classified in the interests of national security.

74. **(U)** Specifically, Wikimedia's Interrogatory Nos. 3-5 ask the Government to describe its understanding of the terms "filtering mechanism," "scanned," and "screened" as used to describe aspects of the Upstream collection process in previous Government filings in this case. The Government did so in its responses to the extent possible without revealing classified operational details about the Upstream collection process. Similarly, Wikimedia's RFA Nos. 6, 8, and 10 ask the Government to admit or deny that the NSA "reviews the contents of Internet communications" in various ways during Upstream surveillance. The Government also responded to these requests to the extent possible without revealing classified information. Wikimedia now insists, however, on disclosures of additional technical details about the "filtering mechanism[s]" employed and the "scann[ing]," "screen[ing]" and content review of communications during Upstream surveillance.

~~TOP SECRET//SI//ORCON/NOFORN~~

75. **(U)** The Government could provide no response to Wikimedia's Interrogatory Nos. 14-15 and RFA Nos. 7, 9, and 37-38, because any response would have required the disclosure of classified operational details about Upstream surveillance. Interrogatory No. 14 asks the Government to describe the entirety of the process by which communications are allegedly copied, filtered, scanned, or otherwise "interacted with" during Upstream collection. Interrogatory No. 15 asks the Government to identify any inaccuracies in the PCLOB's unclassified description of the Upstream collection process, which also would have necessarily required the Government to provide highly technical and classified information about any changes in the sources and methods or operational details of Upstream surveillance since the PCLOB issued its report in July 2014.

76. ~~(TS//SI//NF)~~ [redacted]

[redacted]

[redacted]

77. (~~TS//SI//NF~~) [redacted]

[redacted]

78. (~~S//NF~~) [redacted]

[redacted]

[12] **(U)** As described at greater length in previous filings, *e.g.*, Mem. in Supp. of Defs.' Mot. to Compel, ECF No. 126-1, to send a communication via the Internet, the transmitting device first converts the communication into one or more "packets," relatively small bundles of

[redacted]

79. **(U)** Thus, Wikimedia seeks to compel disclosures concerning classified operational details about the entirety of the Upstream collection process that would reveal to foreign adversaries the NSA's operational methods and capabilities (or lack thereof), enabling them to evade particular types of surveillance and to exploit the NSA's sources and methods of surveillance for their own purposes, in both cases risking exceptionally grave damage to national security.

80. ~~(S//NF)~~ [redacted]

---

digital information. This process is governed by the use of standardized protocols, including, for web pages, the HTTP and HTTPS protocols. Each "packet" is configured with so-called "layers" containing different types of information, some of which provide the address and routing information necessary to send the packet from its origin to its destination over the Internet. The "application layer," by contrast, generally contains a portion of the content of the original communication.

[redacted]

81. (~~TS//SI//NF~~) [redacted]

[redacted]

82. (~~TS//SI//NF~~) [redacted]

[redacted]

83. (~~TS//SI//NF~~) [redacted]

[redacted]

[redacted]

84. (~~S//NF~~) [redacted]

[redacted]

85. (~~S//NF~~) [redacted]

[redacted]

C. (U) Location(s) on the Internet Backbone Where Upstream Surveillance Is Conducted
[Interrogatory Nos. 1, 2; RFA Nos. 13-15, 25-30, 39; RFP Nos. 13, 15, 16, 18, 21, 22]

86. **(U)** I am also supporting the DNI's assertions of privilege and asserting the NSA's statutory privilege over documents and information that would tend to reveal the nature and number of the location(s) on the Internet backbone where Upstream surveillance is conducted.

87. **(U)** As discussed above, the Government has publicly acknowledged that, as part of Upstream surveillance, the NSA collects communications from one or more circuits at one or more points on the Internet backbone. However, to protect sensitive sources and methods of Upstream surveillance, and the identities of assisting electronic communication service providers, the Government has not acknowledged any further details about the number, nature, or specific locations of the sites where Upstream surveillance is conducted.

88. **(~~TS//SI//NF~~)** [redacted]

[redacted]

89. **(U)** Wikimedia Interrogatory No. 2 asks for the Government's understanding of the definition of the term "circuit," as used by the PCLOB in its Section 702 Report. In response to Interrogatory No. 2, the Government has provided an accepted definition of "circuit" as that term is used by the telecommunications industry. The NSA's designated witness also testified that the NSA has no specialized understanding of the term "circuit" that it applies in the context of Upstream surveillance, other than its accepted meaning in the telecommunications industry. In responding, however, to this request for a definition of the term "circuit," the Government has objected to providing classified information about the specific type(s) and/or location(s) of the circuit(s) on which Upstream surveillance is now or in the past has been conducted.

90. **(U)** Wikimedia RFA Nos. 13-15 ask the Government to admit that the NSA conducts Upstream surveillance on "multiple Internet backbone circuits," "multiple international Internet links," and "multiple Internet backbone chokepoints." RFP Nos. 13, 15, and 16 seek documents sufficient to show or estimate the "number of circuits," "number of international Internet links" and the "number of Internet chokepoints" at which Upstream surveillance is conducted.

91. **(~~TS//SI//NF~~)** [redacted]

92. **(U)** Additionally, Wikimedia's request for tens of thousands of pages of classified court orders, opinions, and submissions concerning Upstream surveillance (RFP Nos. 21 and 22) include documents identifying certain telecommunications service providers that at one time or another have been compelled to assist the NSA in Upstream collection activities.

93. **(U)** For the reasons that follow, public release of the documents and information sought by the foregoing could reasonably be expected to cause exceptionally grave damage to national security.

94. **(~~TS//SI//OC/NF~~)**

[redacted]

95. (~~TS//SI//OC/NF~~) [redacted]

96. (~~TS//SI//OC/NF~~) [redacted]

[redacted]

97. (~~TS//SI//OC/NF~~) [redacted]

[redacted]

98. (~~TS//SI//OC/NF~~) [redacted]

[redacted]

[redacted]

99. (~~TS//SI//OC/NF~~) [redacted]

[redacted]

[redacted]

100. (~~TS//SI//NF~~) [redacted]

[redacted]

D. (U) Categories of Internet-Based Communications Subject to Upstream Surveillance Activities
[Interrogatory Nos. 6-8; RFA Nos. 16-18; RFP No. 22]

101. **(U)** I am likewise supporting the DNI's assertions of privilege, and asserting the NSA's statutory privilege, over still-classified documents and information that would reveal or tend to reveal the types of Internet communications that are subject to any stage of the Upstream collection process, and those that are not.

102. **(U)** In this regard, Wikimedia seeks to compel the Government to describe at greater, and classified, length its understanding of the terms "discrete communication," "single communication transaction" and "multi-communication transaction," and of the common features of Internet packets comprising an "Internet transaction." Interrogatory Nos. 6-8. Wikimedia's request that the Government confirm or deny the authenticity of the so-called "NSA slide" headed "Why Are We Interested in HTTP?" also implicates information in this category, as do a significant number of the court submissions concerning Upstream surveillance that are responsive to RFP No. 22. In deposition, Wikimedia also propounded questions to the NSA's designated witness (which she was instructed for reasons of privilege not to answer) concerning the categories of Internet-based communications that are subject to Upstream collection activities, including whether the devices used are configured to exclude various types of encrypted communications.

103. **(~~TS//SI//NF~~)** [redacted]

~~TOP SECRET//SI//ORCON/NOFORN~~

[redacted]

104. (~~TS//SI//NF~~) [redacted]

[redacted]

105. (**U**) So far as Wikimedia's discovery requests in this category are concerned, the first, Interrogatory No. 6, seeks the NSA's understanding of the "definition" of the term "discrete communication" as used in the NSA's 2014 Section 702 Minimization Procedures. Given the innumerable, ever-increasing, and ever-changing means by which to convey information electronically, there is no single, commonly accepted technical definition of a "communication" in the telecommunications industry, and the NSA has not developed a particularized definition of

the term that it uses in connection with Upstream surveillance, or otherwise. Therefore, in responding to Interrogatory No. 6 that the term "discrete communication" means a single communication, the Government has already given the most complete answer to this interrogatory that it is reasonably capable of providing. (To respond in any further detail would require the NSA to reveal the types of communications it collects via Upstream, which inevitably would induce our foreign adversaries to avoid those forms of online communications in order to defeat the NSA's attempts to capture their communications.) So far as Interrogatory No. 8 is concerned, the Government has already responded, straightforwardly that a "single communication transaction" is an Internet transaction containing only a single, discrete communication, and that a "multi-communication transaction" is an Internet transaction that contains multiple discrete communications. (Again, any further response would require the NSA to disclose examples of the kinds of communications it collects today via Upstream—that information is currently and properly classified.) The root of Wikimedia's dissatisfaction with the Government's responses to Interrogatory Nos. 6-8 apparently lies, therefore, with the Government's refusal to provide its understanding, in response to Interrogatory No. 7, of the common features of the Internet "packets" that constitute a single Internet transaction (or communication) for purposes of Upstream surveillance.

106. (~~TS//SI//NF~~) [redacted]

~~TOP SECRET//SI//ORCON/NOFORN~~

[redacted]

107. (~~S//NF~~) [redacted]

[redacted]

108. **(U)** Accordingly, the Government cannot disclose classified information falling within this category, whether in response to Wikimedia's pending discovery requests or otherwise, without risking exceptionally grave damage to the national security of the United States.

E. (U) Scope and Scale of Upstream Surveillance [Interrogatory Nos. 9, 16-19; RFP Nos. 10, 14]

109. **(U)** I am also supporting the DNI's assertions of privilege and asserting the NSA's statutory privilege over still-classified facts concerning the scope and scale of Upstream

surveillance, the disclosure of which would likely motivate foreign adversaries and others to intensify their efforts to avoid such surveillance.

110. **(U)** As discussed above, Wikimedia seeks to compel the Government to reveal the scope of its Upstream surveillance by describing (i) the "body of international communications" that is subject to the surveillance (Interrogatory No. 9); (ii) the approximate percentage of circuits and international submarine cables carrying international Internet traffic into and out of the United States that the NSA is monitoring (Interrogatory Nos. 16-17); and (iii) the approximate amount of Internet traffic subject to each stage of the Upstream process (Interrogatory Nos. 18-19). Wikimedia also seeks the disclosure of documents showing the total bandwidth of the circuits on which Upstream surveillance was conducted, and number of Internet transactions acquired by the NSA, during each of the years 2010-2017 (RFP Nos. 10, 14). These matters were also the subjects of questions propounded by Wikimedia to the NSA's designated deposition witness, which on the basis of privilege the Agency declined to answer.

111. **(~~TS//SI//NF~~)** [redacted]

[redacted]

112. (~~TS//SI//OC//NF~~) [redacted]

113. (~~TS//SI//NF~~) [redacted]

114. (~~TS//SI//NF~~) [redacted]

[redacted]

115. (~~TS//SI//NF~~) [redacted]

[redacted]

116. (~~TS//SI//NF~~) [redacted]

[redacted]

F. (~~S//NF~~) NSA's Capabilities, or Lack Thereof, to Decrypt, Circumvent, or Defeat Communications Security Protocols
[Interrogatory No. 20; RFA No. 40]

117. (~~TS//SI//NF~~) [redacted]

[redacted]

[redacted]

118. **(U)** In particular, Wikimedia's Interrogatory No. 20 asks the Government to describe any Internet Protocols subject to Upstream surveillance that the NSA is able to decrypt. RFA No. 40 asks a related but narrower question: whether the NSA has the ability to decrypt any portion of HTTPS communications that may be subject to Upstream surveillance. Wikimedia asked similar questions during the deposition of the NSA's designated witness.

119. **(~~TS//SI//NF~~)** [redacted]

120. **(~~TS//SI//NF~~)** [redacted]

[redacted]

G. (U) Additional Categories of Classified Information Contained in Opinions, Orders, and Court Submissions Concerning Upstream Surveillance [RFP Nos. 21-22]

121. **(U)** Finally, as discussed herein, Wikimedia RFP Nos. 21 and 22 ask the Government to produce all FISC, Foreign Intelligence Surveillance Court of Review, and Supreme Court opinions and orders concerning Upstream surveillance, and all submissions to these courts concerning Upstream surveillance, since the enactment of Section 702 in 2008.[13] I am also supporting the DNI's assertions of privilege, and asserting the NSA's statutory privilege, over the additional categories of classified information contained in the more than 10,000 pages of documents responsive to RFP Nos. 21 and 22.

122. **(~~TS//SI//NF~~)** [redacted]

[13] **(U)** As noted earlier, neither the Foreign Intelligence Court of Review, nor the Supreme Court, has issued any opinions or orders, nor has the Government made any filings in either court, concerning Upstream surveillance.

[redacted]

123. (~~TS//SI//NF~~) [redacted]

[redacted]

124. (~~TS//SI//NF~~) [redacted]

[redacted]

[redacted]

125. (~~TS//SI//NF~~) [redacted]

[redacted]

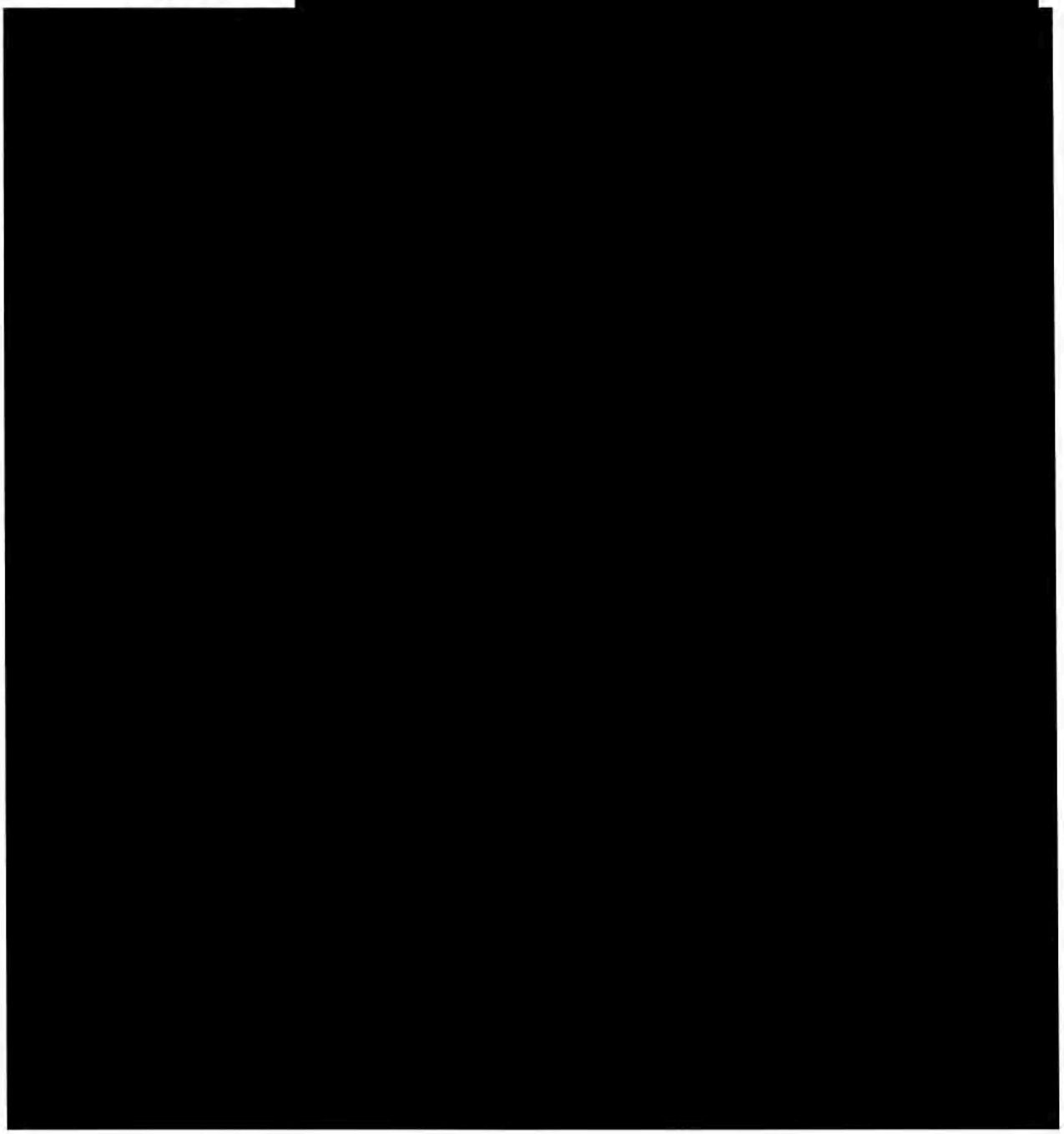
126. (~~TS//SI//NF~~) [redacted]

[redacted]

127. (~~TS//SI//NF~~) [redacted]

[redacted]

128. (~~S//OC//NF~~) [redacted]



129. (U) For the reasons discussed above, disclosure of the aforementioned categories of classified information contained in documents responsive to Wikimedia's RFP Nos. 21 and 22

could reasonably be expected to cause exceptionally grave harm to the national security of the United States.

VII. (U) CONCLUSION

130. **(U)** Set forth in this declaration is the NSA's support for the assertion by the DNI of the state secrets privilege, of the statutory privilege under 50 U.S.C. § 3024(i)(1), and the NSA's assertion herein of the privilege under 50 U.S.C. § 3605(a), over the foregoing seven categories of classified information, whether sought in response to Wikimedia's pending discovery requests, in response to any future discovery requests Wikimedia may serve in this case, or as otherwise may become necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this case. The information contained in the above-described categories concerns critical NSA intelligence-gathering functions, is classified, and extraordinarily sensitive. Its disclosure could cause exceptionally grave damage to the national security of the United States. For the reasons explained above, I therefore support the assertion by the DNI of the state secrets privilege over this information, of the statutory privilege under 50 U.S.C. § 3024(i)(1), and I assert NSA's privilege under Section 6 of the National Security Agency Act, 50 U.S.C. § 3605(a).

~~TOP SECRET//SI//ORCON/NOFORN~~

I declare under penalty of perjury, pursuant to 28 U.S.C § 1746, that the foregoing is true and correct to the best of my knowledge and belief.

Executed on April 24, 2018

[redacted]

GEORGE C. BARNES, Deputy Director
National Security Agency

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, *Plaintiff*, v. NATIONAL SECURITY AGENCY / CENTRAL SECURITY SERVICE, *et al.*, *Defendants*.	Civil Action No. 15-cv-00662-TSE

DECLARATION OF ASHLEY GORSKI IN SUPPORT OF PLAINTIFF WIKIMEDIA FOUNDATION'S MOTION TO COMPEL

I, Ashley Gorski, a member of the Bar of the State of New York and admitted *pro hac vice* to the Bar of this Court, declare under penalty of perjury as follows:

1. I am an attorney with the American Civil Liberties Union Foundation, and represent Plaintiff Wikimedia Foundation in this matter. I submit this declaration in support of Plaintiff's Motion to Compel.

2. Attached hereto as **Exhibit 1** is a chart identifying the questions from the April 16, 2018 deposition of Defendant National Security Agency on which Plaintiff is moving to compel testimony.

3. Attached hereto as **Exhibit 2** is a true and correct copy of the redacted transcript of the April 16, 2018 deposition of Defendant National Security Agency's designated witness, Rebecca J. Richards, pursuant to Federal Rule of Civil Procedure 30(b)(6).

* * *

I declare under penalty of perjury that the foregoing is true and correct.

Ashley Gorski

Date: May 18, 2018
New York, New York

Exhibit 1

Wikimedia Foundation v. National Security Agency et al.
No. 15 Civ. 00662 (TSE)

Transcript Citations

Deposition of NSA Rule 30(b)(6) Witness Rebecca J. Richards

The deposition questions fall into the three categories that Wikimedia identified in its opening brief, Pl. Br. 3–8, plus one additional category:

Category 1: Direct evidence that Wikimedia has been surveilled.[1]

Category 2: The meanings and definitions of key terms the government has used to describe Upstream surveillance to the public.

Category 3: Evidence concerning the scope and breadth of Upstream surveillance.

Category 4: Evidence rebutting speculation and hypotheticals that the government's outside expert intends to offer concerning Upstream surveillance. *See* Def. Mot. to Compel 11–14 (ECF No. 126-1).

Depending on how the Court chooses to structure its in camera review—for instance, by prioritizing straightforward admissions about the surveillance, or based on the assistance and input of the Court's own expert—Wikimedia will identify any subset(s) of questions that the Court may request.

No.	Category 1 Excerpted Questions: Direct Evidence That Wikimedia Has Been Surveilled	Citation to Questions and Context
1.	Does NSA now scan Wikimedia's communications in the course of Upstream surveillance?	Tr. 328:15-17
2.	In 2015, did NSA scan Wikimedia communications in the course of upstream surveillance?	Tr. 329:3-5
3.	Does NSA now copy Wikimedia communications in the course of upstream surveillance?	Tr. 329:11-13
4.	In June 2015, did NSA copy Wikimedia communications in the course of upstream surveillance?	Tr. 329:19-21
5.	Has NSA acquired Wikimedia communications as a result of upstream surveillance now?	Tr. 330:5-7

[1] Several questions in Category 4 also concern surveillance of Wikimedia specifically.

6.	As of June 2015, had NSA acquired Wikimedia communications as a result of upstream surveillance?	Tr. 330:13-15
7.	If you assumed that Exhibit 54 related to upstream surveillance, it would indicate, wouldn't it, that the NSA had an intelligence interest in Wikimedia's communications, wouldn't it? (Referring to Deposition Exhibit 54, NSA slide titled, "Why Are We Interested in HTTP?")	Tr. 331:15-19
8.	What is [Exhibit 55]? (Referring to Deposition Exhibit 55, NSA slide titled, "Fingerprints and Appids")	Tr. 333:11
9.	If you assumed that Exhibit 55 related to upstream surveillance, it would indicate, wouldn't it, particularly on the second page in the first bullet point, that the NSA has an intelligence interest in Wikimedia's HTTP communications, wouldn't it? (Referring to Deposition Exhibit 55, NSA slide titled, "Fingerprints and Appids")	Tr. 333:19-334:2
10.	Do Exhibits 54 or 55 relate to upstream surveillance? (Referring to Deposition Exhibit 54, Slide titled, "Why Are We Interested in HTTP?," and Deposition Exhibit 55, NSA slide titled, "Fingerprints and Appids")	Tr. 334:8-9

No.	**Category 2 Excerpted Questions:** **The Meanings and Definitions of Key Terms**	**Citation to Questions and Context**
1.	What do you understand the Foreign Intelligence Surveillance Court to mean in its use of the term "international Internet link" in that sentence? (Referring to Deposition Exhibit 45, page 45, [*Redacted*], No. [Redacted], 2011 WL 10945618, at *15 (FISC Oct. 3, 2011): "Indeed, the government readily concedes that NSA will acquire a wholly domestic 'about' communication if the transaction is routed through an international Internet link being monitored by NSA or is routed through a foreign server.")	Tr. 160:19-22

2.	Is the NSA's understanding of the term ["international Internet link"] different from the general meaning of the term you described in response to an earlier question as a link between two countries?	Tr. 162:2-6
3.	Is it your understanding that an international Internet link is an Internet backbone circuit with one end in the United States and the other end in a foreign country?	Tr. 163:2-5
4.	In the context of upstream surveillance, can you tell me what an international chokepoint is?	Tr. 183:17-19
5.	[W]ith respect to upstream surveillance as it operated in 2015, . . . what other processes could be used to accomplished either the filtering or the screening described in the sentence you were reading from page 37 of Exhibit 43? (Referring to Deposition Exhibit 43, Referring to Deposition Exhibit 43, Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of FISA* 37(2014), https://perma.cc/J3DZ-62HL ("PCLOB Report"): "Internet transactions are first filtered to eliminate potential domestic transactions, and then are screened to capture only transactions containing a task selector.")	Tr. 200:20-201:4
6.	Can an Internet protocol address be a selector under upstream surveillance?	Tr. 206:19-20
7.	Can a URL, or uniform resource locator, be a selector under upstream surveillance?	Tr. 207:6-8
8.	Could a URL be a selector under upstream surveillance as of June 2015?	Tr. 208:6-7
9.	What does "web activity" mean in the context of Internet communications?	Tr. 222:14-15
10.	Would Internet web browsing constitute web activity? (Referring to Deposition Exhibit 47, page 30, June 1, 2011 FISC Submission, attached as Toomey Decl., Ex. 25 (ECF No. 125-28))	Tr. 223:19-20
11.	I'm asking because your answer suggested that you believe "web activity" to be essentially used interchangeably with the very generic term "Internet traffic" or "Internet	Tr. 227:14-21

	communications," and I would assume, if that were the case, then the NSA would in fact use that term interchangeably, but I don't believe that to be the case. I'm asking why that is.	
12.	Are the filtering or screening processes that you've described under upstream surveillance as conducted in June 2015 forms of deep packet inspection?	Tr. 244:18-21
13.	Do the Internet packets that constitute a single Internet transaction have a common destination?	Tr. 254:4-6
14.	Do the Internet packets that constitute a single Internet transaction have a common source?	Tr. 254:20-22
15.	Is an Internet transaction, as understood by the NSA, the same as a flow or network flow as used in the context of Internet communications?	Tr. 255:15-257:19

No.	**Category 3 Excerpted Questions:** **Evidence Concerning the Scope and Breadth of Upstream**	**Citation to Questions and Context**
1.	As of 2014, did the NSA conduct upstream surveillance on more than one Internet backbone circuit?	Tr. 123:7-9
2.	As of 2014, were multiple electronic communication service providers compelled to assist the NSA in the operation of upstream surveillance?	Tr. 126:7-128:4
3.	Can you tell us whether there have been more than one provider involved, even if not more than one at the same time?	Tr. 128:22-129:2
4.	Do you understand this sentence to confirm that service providers are compelled to assist NSA in the lawful interception of electronic communications to, from, or about task selectors as of April 16th, 2014? (Referring to Deposition Exhibit 44, NSA Director Report 5: "[S]ervice providers are compelled to assist NSA in the lawful interception of electronic communications to, from, or about tasked selectors.")	Tr. 132:7-133:13
5.	What is the number, or approximate number, of Internet backbone circuits on which upstream surveillance is	Tr. 145:14-18

	conducted . . . as of June 2015?	
6.	What is the number, or approximate number, of Internet backbone circuits on which upstream surveillance is conducted today?	Tr. 146:10-12
7.	What is the approximate combined bandwidth of the Internet backbone circuits on which upstream surveillance was conducted in June of 2015?	Tr. 147:12-15
8.	What is the approximate combined bandwidth of the Internet backbone circuits on which upstream surveillance is conducted today?	Tr. 147:21-148:1
9.	What are the categories of circuits that were subject to upstream surveillance in June 2015?	Tr. 148:6-8
10.	What are the categories of circuits that are subject to upstream surveillance today?	Tr. 148:13-14
11.	Does the NSA conduct upstream surveillance on one or more international Internet links?	Tr. 180:2-5
12.	Did the NSA conduct upstream surveillance on one or more international Internet links in 2015?	Tr. 180:16-8
13.	Does the NSA conduct upstream surveillance today on more than one international Internet links?	Tr. 181:2-4
14.	Did the NSA conduct upstream surveillance on more than one international Internet links in June of 2015?	Tr. 181:10-12
15.	What is the number or approximate number of international Internet links on which the NSA conducted upstream surveillance in June of 2015?	Tr. 181:17-20
16.	What is the approximate number of international Internet links on which the NSA today conducts upstream surveillance?	Tr. 182:4-6
17.	Is upstream surveillance conducted on any international submarine cables?	Tr. 182:11-12
18.	Was upstream surveillance conducted on any international submarine cables in June of 2015?	Tr. 182:18-20
19.	What is the number or approximate number of cables on which the NSA conducted upstream surveillance in June	Tr. 183:3-5

	2015?	
20.	What is the number or approximate number of cables on which the NSA today conducts upstream surveillance?	Tr. 183:10-12
21.	Is upstream surveillance today conducted at one or more international chokepoints?	Tr. 184:6-8
22.	Was upstream surveillance in June 2015 conducted at one or more international chokepoints?	Tr. 184:13-15
23.	What number, approximate number, of international chokepoints was upstream surveillance conducted on in June 2015?	Tr. 184:21-185:1
24.	What number, approximate number, of international chokepoints is upstream surveillance conducted on today?	Tr. 185:6-8
25.	As of October 3rd, 2011, did the NSA conduct upstream surveillance on one or more international Internet links?	Tr. 186:11-13
26.	Do you understand th[at] sentence . . . to confirm that, as of October 3rd, 2011, that the government in fact conducted upstream surveillance at at least one international Internet link? (Referring to Deposition Exhibit 45, page 45, [*Redacted*], No. [Redacted], 2011 WL 10945618, at *15 (FISC Oct. 3, 2011): "Indeed, the government readily concedes that NSA will acquire a wholly domestic 'about' communication if the transaction is routed through an international Internet link being monitored by NSA or is routed through a foreign server.")	Tr. 187:15-20
27.	Can you tell us what those certain circumstances would be in unclassified terms? (Referring to Deposition Exhibit 44, NSA Director Report 5: "In certain circumstances, NSA's procedures require that it employ an Internet protocol filter to ensure that the target is located overseas.")	Tr. 194:15-16
28.	Are all transactions that were subject to upstream surveillance in June 2015 subjected to Internet protocol filtering . . . to eliminate potential domestic transactions from upstream surveillance?	Tr. 201:12-20
29.	Could you please describe all the ways in which the NSA	Tr. 202:17-20

	could determine in 2015, as part of upstream surveillance, whether a transaction is wholly domestic so as to filter it out?	
30.	Were the selectors used for upstream surveillance the same as those used for PRISM surveillance in June 2015?	Tr. 208:21-209:3
31.	As of 2015, did the procedures approved by the FISC for upstream surveillance permit the NSA to collect an international HTTP transmission of a website if the text of that website contained a selector?	Tr. 219:10-14
32.	[D]id the NSA, in June of 2015, have the authority to collect the communications of a foreign target abroad with a website in the United States?	Tr. 234:5-8
33.	[U]nder upstream surveillance as conducted in 2015, did the NSA have the authority to collect the transactions of a foreigner abroad with a website in the United States if the website contained a selector task for collection?	Tr. 234:17-21
34.	Has the NSA collected webmail in-boxes as part of upstream surveillance?	Tr. 242:10-11
35.	[I]n the course of upstream surveillance, does the NSA review the contents of communications as they are in transit on the Internet backbone?	Tr. 258:15-18
36.	In the course of upstream surveillance in June 2015, did the NSA review the contents of communications as they were in transit on the Internet backbone?	Tr. 259:6-9
37.	In the course of upstream surveillance in June 2015, did the NSA scan the contents of communications as they were in transit on the Internet backbone?	Tr. 259:20-260:1
38.	[I]n June 2015, did the NSA scan the application layer data of communications that transit the Internet backbone? . . . When you say certain . . . application layer data, what you mean by "certain"?	Tr. 263:10-264:1
39.	Today does the NSA scan the application layer data of communications that transit the Internet backbone?	Tr. 266:5-7
40.	In June of 2015, if a transaction was scanned by the NSA in the course of upstream surveillance, and the NSA determined that it did not contain a selector, was the communication eliminated?	Tr. 266:15-19

41.	Today, does the NSA seek to acquire email communications to and from its targets using upstream surveillance?	Tr. 268:15-17
42.	Could you please describe as fully as possible how, in June 2015, the NSA determined whether an Internet transaction contained a selector?	Tr. 269:3-6
43.	Beyond what you've already said or what appears in the NSA's discovery responses, could you please describe as fully as possible how the NSA today determines whether an Internet transaction contains a selector?	Tr. 269:18-22
44.	In the course of upstream surveillance in June 2015, did the NSA scan communications in bulk?	Tr. 270:14-273:9
45.	In the course of upstream surveillance today, does the NSA scan communications in bulk?	Tr. 274:8-9
46.	In the course of upstream surveillance today, does the NSA scan the metadata of communications in bulk?	Tr. 274:16-18
47.	In the course of upstream surveillance in 2015, did the NSA copy communications in bulk?	Tr. 275:2-3
48.	In the course of upstream surveillance today, does the NSA copy communications in bulk?	Tr. 275:8-9
49.	Would the NSA be permitted under upstream surveillance today to collect a target[']s communications with a U.S.-based website?	Tr. 284:4-6
50.	Can you please describe in as much detail as necessary to provide a complete answer how the NSA implemented any changes to "about" collection during or after April 2017?	Tr. 293:18-296:5
51.	[C]ould you please describe in as much detail as necessary to provide a complete answer how, after April 2017, the NSA attempts to avoid collecting communications that are solely about a selector?	Tr. 296:21-298:6
52.	[P]lease describe in as much detail as necessary to provide a complete answer how the change in April 2017 affected the filtering of communications subject to upstream surveillance?	Tr. 298:7-13
53.	[C]ould you please describe in as much detail as necessary to give a complete answer how the change in April 2017 affected the scanning of communications subject to upstream	Tr. 299:20-300:2

	surveillance?	
54.	[P]lease describe in as much detail as necessary to give a complete answer which portions of an Internet transaction are scanned for selectors after April 2017?	Tr. 300:10-14
55.	Since April 2017, does the NSA first scan the contents of communications for selectors, and then discard those that are solely about a selector?	Tr. 300:20-301:1
56.	Since April 2017, does the NSA copy the contents of communications prior to scanning those communications?	Tr. 301:9-11
57.	Since April 2017, does the NSA copy the application layer data of packets prior to scanning the communications to which they belong?	Tr. 301:17-19
58.	Since April 2017, does the NSA review any portion of the contents of communications for selectors?	Tr. 302:3-5
59.	Since April 2017, does the NSA scan any portion of the contents of Internet transactions for selectors?	Tr. 303:5-7
60.	[W]hat portions of the contents of Internet transactions are scanned for selectors since April 2017?	Tr. 304:13-15
61.	Since April 2017, does the NSA scan the entire contents of Internet transactions for selectors?	Tr. 305:13-15
62.	Since April 2017, does the NSA scan any portion of the application layer data of Internet transactions for selectors? . . . And if I were to ask what portions of Internet transaction the NSA scans for selectors, would your answer be the same?	Tr. 306:2-15
63.	[S]ince April 2017, does the NSA scan the entire application layer of Internet transactions for selectors?	Tr. 306:21-307:1
64.	Are there any barriers to the NSA restarting "about" collection today? . . . [A]re there any other barriers besides the two that you just described? . . . What are those underlying issues? . . . And what were those issues?	Tr. 307:7-311:17
65.	Besides the barriers you already identified and what's described in Exhibit 51, are there any other barriers to the NSA restarting "about" collection? (Referring to Deposition Exhibit 51, FISC Opinion dated	Tr. 313:17-20

	April 26, 2017, attached as Toomey Decl., Ex. 29 (ECF No. 125-32))	
66.	Has the NSA indicated to the FISC any interest in resuming "about" collection in the future?	Tr. 316:20-22
67.	Has the NSA indicated to the FISC that it intends to resume "about" collection in the future?	Tr. 317:13-15
68.	Today, does upstream surveillance involve the scanning of all international text-based communications on [the] individual circuit or circuits the NSA is monitoring?	Tr. 322:16-19
69.	In June 2015, did upstream surveillance involve the scanning of all international text-based communications on the individual circuit or circuits the NSA was monitoring?	Tr. 324:7-11
70.	Today, if some international text-based communications on a given circuit are not scanned, please explain in as much detail as necessary to completely answer why those communications are not scanned . . . [C]an you please fully explain in as much detail as necessary why some communications are not scanned?	Tr. 324:17-326:2
71.	[A]s of June 2015, if some international text-based communications on a given circuit were not scanned, please explain in as much detail as necessary to fully answer why those communications are not scanned.	Tr. 326:13-328:2
72.	At this time, HTTP communications are scanned for selectors in the course of upstream surveillance, aren't they?	Tr. 334:15-17
73.	As of June 2015, HTTP communications were scanned for selectors in the course of upstream surveillance, right?	Tr. 335:14-16
74.	At this time, HTTPS communications are scanned for selectors in the course of Upstream surveillance, aren't they? . . . Same question as to the June 2015 time frame.	Tr. 335:22-336:9
75.	Are Apache Kafka communications scanned for selectors in the course of upstream surveillance?	Tr. 336:15-17
76.	Open VPN communications are scanned for selectors in the course of upstream surveillance, aren't they?	Tr. 337:11-13
77.	As of June 2015, were open VPN communications scanned for selectors in the course of upstream surveillance?	Tr. 337:21-338:1

78.	Other than public documents, public documents at large, hearing testimony that is transcribed, public documents you reviewed, documents that have been filed or served in this case, or your testimony today, what can you tell me about the volume of communications subject to upstream surveillance at this time using any unit of measurement you want to discuss volume of communications?	Tr. 338:8-16
79.	How many communications -- and you can use any unit of measurement you want -- did NSA retain as a result of upstream surveillance in each of the last three years?	Tr. 339:14-17
80.	What is the volume of communications copied in the course of upstream surveillance in each of the last three years? . . . Same question as to transactions.	Tr. 340:9-19
81.	What is the volume of communications or transactions that are subject to filtering in the course of upstream surveillance in the last three years?	Tr. 341:3-6
82.	[I]t's accurate . . . to say that upstream surveillance, as of June 2015, involved deep packet inspection, right?	Tr. 349:5-7
83.	Today, how many targets does NSA have for upstream surveillance?	Tr. 349:20-350:8
84.	In June 2015, how many targets did NSA have for upstream surveillance?	Tr. 351:3-4
85.	What's inaccurate about the sentence at the bottom of page 36, carrying over onto page 37, in Exhibit 43? (Referring to Deposition Exhibit 43, PCLOB Report 36–37: "Once tasked, selectors used for the acquisition of upstream Internet transactions are sent to a United States electronic communication service provider to acquire communications that are transiting through circuits that are used to facilitate Internet communications, what is referred to as the "Internet backbone.")	Tr. 110:4-112:3
86.	Is [the sentence] inaccurate as to the operation of upstream surveillance today? (Referring to Deposition Exhibit 43, PCLOB Report 36–37, quoted above)	Tr. 115:8-22

No.	Category 4 Excerpted Questions: Evidence Rebutting Defendants' Hypotheticals	Citation to Questions and Context
1.	In the course of upstream surveillance in June of 2015, did the NSA deliberately attempt to filter out any of Wikimedia's international communications?	Tr. 275:14-17
2.	In the course of upstream surveillance today, does the NSA deliberately attempt to filter out any of Wikimedia's international communications?	Tr. 276:2-5
3.	In the course of upstream surveillance in June of 2015, did the NSA deliberately attempt to filter out all of Wikimedia's communications?	Tr. 276:10-12
4.	In the course of upstream surveillance today, does the NSA deliberately attempt to filter out all Wikimedia communications?	Tr. 276:17-19
5.	Does the NSA contend as a factual matter in this case that it deliberately filters out all Wikimedia communications?	Tr. 277:3-5
6.	Does anyone at the NSA know whether the NSA contends in this case, as a factual matter, that it deliberately filters out all Wikimedia communications?	Tr. 278:2-279:3
7.	Has the NSA programmed its surveillance equipment to disregard HTTPS communications altogether?	Tr. 281:1-3
8.	Does the NSA have the ability to decipher HTTPS communications?	Tr. 281:13-282:9
9.	Has the NSA configured its surveillance equipment to ignore all communications having source or destination IP addresses associated with Wikimedia?	Tr. 282:18-283:10
10.	Does the NSA deem communications to and from Wikimedia's website to be of low foreign intelligence value?	Tr. 283:19-21
11.	Could the term "foreign intelligence information" encompass information that a person surveilled using Upstream surveillance is reading on one of Wikimedia's websites?	Tr. 286:5-8
12.	[C]ould the term "foreign intelligence information" encompass information that a person surveilled using upstream surveillance is contributing to one of Wikimedia's	Tr. 288:4-289:18

	websites? . . . Could you please provide any classified information that you believe my question calls for?	
13.	Today, does the NSA intentionally attempt to filter out all HTTPS communications from upstream surveillance?	Tr. 290:6-8
14.	[In] June 2015, [d]id the NSA at that time intentionally attempt to filter out all HTTPS communications from upstream surveillance?	Tr. 290:16-19
15.	Today, does the NSA intentionally attempt to filter out all Internet communications that use TCP port 443?	Tr. 291:3-5
16.	In June 2015, did the NSA intentionally attempt to filter out all Internet communications that used TCP port 443?	Tr. 291:10-12
17.	Today, does the NSA intentionally filter out all encrypted VPN communications?	Tr. 291:17-18
18.	In June 2015, did the NSA intentionally filter out all encrypted VPN communications?	Tr. 292:2-4
19.	Today, does the NSA intentionally filter out all open VPN communications?	Tr. 292:9-10
20.	In June 2015, did the NSA intentionally filter out all open VPN communications?	Tr. 292:15-17
21.	Today does the NSA intentionally filter out Wikimedia's encrypted VPN communications?	Tr. 293:2-4
22.	In June 2015, did the NSA intentionally filter out Wikimedia's encrypted VPN communications?	Tr. 293:10-12

Exhibit 2

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, Plaintiff, vs. NATIONAL SECURITY AGENCY, et al., Defendants.	Case No. 1:15-cv-00662-TSE

Deposition of REBECCA J. RICHARDS

Monday, April 16, 2018

Washington, D.C.

Reported by:

Dawn A. Jaques

Job no: 21368

Deposition of:

REBECCA J. RICHARDS,

the witness, was called for examination by counsel for the Plaintiffs, pursuant to notice, commencing at 9:12 a.m., at the offices of the Department of Justice, Civil Division, Federal Programs Branch, 20 Massachusetts Avenue, Northwest, Washington, D.C., before Dawn A. Jaques, CSR, CLR, and Notary Public in and for the District of Columbia.

APPEARANCES:

On behalf of the Plaintiffs:

ALEX ABDO, ESQ.
Knight First Amendment Institute
535 West 116th Street
314 Low Library
New York, New York 10027
PHONE: (212) 854-1128
EMAIL: alex.abdo@knightcolumbia.org

- AND -

DEVON HANLEY COOK, ESQ.
Cooley LLP
101 California Street, 5th Floor
San Francisco, CA 94111-5800
PHONE: (415) 693-2116
EMAIL: dhanleycook@cooley.com

ALSO PRESENT on behalf of Plaintiffs:

Patrick Toomey, Esq., ACLU
Ashley Gorski, Esq., ACLU

APPEARANCES (Continued):

On behalf of the Defendants:

RODNEY PATTON, ESQ.
JAMES J. GILLIGAN, ESQ.
U.S. Department of Justice
Civil Division
Federal Programs Branch
20 Massachusetts Avenue, N.W.
Washington, D.C. 20530
PHONE: (202) 305-7919 (Mr. Patton)
(202) 514-3358 (Mr. Gilligan)
EMAIL: rodney.patton@usdoj.gov
james.gilligan@usdoj.gov

ALSO PRESENT FROM THE NATIONAL SECURITY AGENCY:

JASON PADGETT, ESQ.
KATHLEEN [redacted]
(443) 479-2613
[redacted]
MARY [redacted]
(301) 688-6054
[redacted]

I-N-D-E-X

E-X-H-I-B-I-T-S

INDEX (Continued)

E-X-H-I-B-I-T-S

INDEX (Continued)

E-X-H-I-B-I-T-S

P R O C E E D I N G S

MR. ABDO: Good morning, Ms. Richards. My name is Alex Abdo, and I'm here with the Knight First Amendment Institute and Columbia University, representing the Plaintiff in this case, Wikimedia Foundation.

I think you met everyone down the line, but I'm joined by my colleagues, Patrick Toomey from the American Civil Liberties Union; Devon Hanley Cook from Cooley LLP; and Ashley Gorski, also from the American Civil Liberties Union.

Would you just start out by stating your full name for the record and spelling it for us?

MR. PATTON: Could we just before we begin introduce the other attorneys here just for the record?

MR. ABDO: Please, yeah.

MR. PATTON: I'm Rodney Patton with the Department of Justice representing the NSA.

MR. PADGETT: Jason Padgett, the

Office of General Counsel at the National Security Agency.

MR. GILLIGAN: James Gilligan with the DOJ representing the defendants.

MS. [redacted] Mary [redacted] with the Office of General Counsel at the National Security Agency.

MS. [redacted] And Cathleen [redacted], Office of General Counsel, National Security Agency.

MR. ABDO: Great, I think we're done with appearances.

Ms. Richards, would you just state your full name and spell it for the record?

THE WITNESS: Rebecca Joan Richards, R-E-B-E-C-C-A, J. Richards, R-I-C-H-A-R-D-S.

MR. PATTON: This is Rodney Patton on behalf of Defendants in the case. The parties have agreed to the following rules governing the taking of this deposition.

One, counsel for the government may make such objections as he deems in good faith to

be necessary to prevent the unauthorized disclosure of protected, classified, or privileged information.

Two, counsel for the government may at any time direct the witness not to answer a question or to stop responding to a question if he deems it in good faith that it is necessary to prevent the unauthorized disclosure of protected, classified, or privileged information.

Number three, counsel for the government or the witness may stop the deposition at any time in order to confer privately in a Secure Compartmented Information Facility, known as a SCIF, for the purpose of preventing the unauthorized disclosure of protected, classified, or privileged information.

Four, nothing in the testimony of the witness will constitute or be construed as a waiver of the applicable protections or privileges subject to the plaintiffs -- or subject to the NSA reviewing the transcript.

Five, during the deposition, the

transcript may be displayed only on the court reporter's laptop, and it will not be otherwise transferred to or displayed on anyone else's electronic device during the deposition.

Six, after the deposition, the transcript will be transferred from the court reporter's laptop to counsel for the NSA by a CD or flash drive.

Seven, the transcript of the deposition will not otherwise be copied, except as appropriate by the NSA, or transmitted from the court reporter's laptop until counsel for the NSA provides the Agency's approval to do so.

Finally, in the meantime, the NSA will conduct a review of the transcript for protected, privileged, and classified information, and will redact any such information prior to the release of the transcript to plaintiff's counsel, or anyone other than the NSA and the court reporter.

That's all the ground rules. Thank you.

MR. ABDO: Ms. Jaques, have you sworn

Ms. Richards in? Would you mind doing so?

THE REPORTER: Raise your right hand, ma'am.

(The witness was administered the oath.)

Whereupon,

REBECCA J. RICHARDS,

was called as a witness, after having been first duly sworn by the Notary Public, was examined and testified as follows:

EXAMINATION BY COUNSEL FOR PLAINTIFF

BY MR. ABDO:

Q Ms. Richards, you understand that you're here today to give deposition testimony in the lawsuit of Wikimedia Foundation versus NSA, right?

A Yes.

Q And you understand that you're under oath?

A Yes.

Q Have you been deposed before?

A No.

Q Okay. So you heard a portion of the

procedures described by your counsel, Mr. Patton. I'll go over some other procedures for how the deposition will take place.

So we'll be asking you questions. Our questions and your answers will be recorded by Ms. Jaques. For that reason, it's important that you speak up and give your answers orally so that Ms. Jaques can record them, transcribe them. She won't be able to record a nod or a shake of the head.

Now, I may on occasion ask you a question that isn't clear, or that for some other reason you don't understand. If you don't understand one of my questions, let me know. It's my job to ask you clear questions. So if you say you don't understand one, I'll try to make it clearer. Do you understand that?

A Yes, I do.

Q Good. Your counsel may object at various points. If he does, please go ahead and answer the question that has been objected to unless your counsel specifically instructs you not

to answer. Do you understand that?

A Yes, I do.

Q We'll be taking periodic breaks during the deposition, but if you need to take a break at any other point, let us know. We will accommodate you. And I think you see that there's some water and coffee in the corner. If you need anything, just help yourself at any point during the deposition.

If at any point you realize that an answer you've given is incomplete or inaccurate and you'd like to supplement it or correct it in any way, let me know right away and we'll take care of it right then. Does that sound okay?

A Yes.

Q And if at any point in answering our questions you think of a document that would be helpful in refreshing your recollection, in answering the question, or in recalling what has been publicly disclosed and what hasn't about upstream surveillance, please tell us. We likely have many of those documents here today and would

be happy to provide you them. Is that okay?

A Yes, it is.

Q Great. So your counsel, Mr. Patton, outlined the process that the parties have agreed to for addressing objections based on information the NSA believes to be subject to the state secrets privilege or protected from disclosure under 50 U.S.C. § 3024(i)(1) and/or 50 U.S.C. § 3605(a). We will adhere to that process.

I'm going to use the term "classified" to refer to information the NSA believes is protected by any of those legal authorities. Is that okay with you --

A Yes.

Q -- that shorthand?

MR. PATTON: Can we just state for the record that not all of the information that will be protected by 3605, for example, is necessarily classified, but I understand your shorthand.

BY MR. ABDO:

Q Please take your time when answering

our questions. Our goal is not to trick you into disclosing protected information. We have a process in place to address those sorts of claims, but for that process to work, we need to make a clear record concerning any information the NSA believes is classified.

There are at least three scenarios that may arise. First, if you can answer a question fully without disclosing information that the NSA believes to be classified, you must do so.

Second, if you believe that a response to a question would disclose information the NSA considers classified, you should clearly state that for the record.

And, third, if you believe that a question calls for a response that is classified in part and unclassified in part, please also state that clearly for the record. You must answer and provide the unclassified information even if that does not constitute a complete response because there is also unclassified information.

Do you understand those three scenarios?

A Yes, I do.

Q Now, this case concerns surveillance that has taken place from 2015 to the present. Unless I say otherwise, my questions will apply to that full period.

If your answer would differ based on what specific portion of that period we're talking about, please say so, and please explain how it would differ for the relevant time frames.

We will do our best to make clear what time frame we're talking about, and then I'm sure your counsel will make sure we're making clear what time frame we're talking about, but if we haven't specified, please do your best to answer with respect to the full period.

Is there any reason you can think of why you would not be able to answer our questions fully and accurately today?

A No.

MR. PATTON: Other than that the

answers may be classified.

THE WITNESS: Yeah.

BY MR. ABDO:

Q Sorry, sorry. I mean are you taking any medications or drugs that would make it difficult for you to answer truthfully or accurately?

A No.

Q There's nothing that is affecting your memory today?

A No.

Q Okay. You stated before that you have not been deposed before; is that correct?

A That's correct.

Q Have you ever given testimony in a case?

A No, I have not.

Q Okay. You understand that you're appearing here today as a designated representative of the NSA, right?

A Yes.

(Deposition Exhibit 41 was marked for identification.)

BY MR. ABDO:

Q So you have in front of you what's been marked as Exhibit 41. Do you recognize that document marked as 41?

A Yeah.

Q What is it?

A These are the topics for examination. Do you want me to read more fully?

Q No, no, no.

A How detailed would you like me to be?

Q I'm asking whether that's the deposition notice that the plaintiff served on the defendants in this case.

A Oh, yes, it is. Sorry.

Q And you're appearing here today as a designee of the NSA on topics 2, 3, 4a, 4d and 6 as set forth in Exhibit 41; is that correct?

A Yes, that is correct.

Q Are you prepared to testify today about those topics?

A Yes, I am.
Q Can you tell us what you did to prepare?
A Reviewed the documents submitted, as well as a number of different documents that are already in the unclassified realm, ranging from previous minimization procedures, the NSA Civil Liberties and Privacy Office Report, the Privacy and Civil Liberties Oversight Board's report on 702, FISC opinions, as well as NSA's submissions at different points to the FISC.
Q The FISC opinions that you reviewed, are those all ones that have been disclosed publicly?
A Yes. I only reviewed the unclassified versions, so the redacted versions that are readily available on ODNI's website.
Q Did you also review any classified FISC opinions or other documents in preparing for today's deposition?
A No. We met with a subject -- I met with a subject matter expert. We discussed what

was classified and what was not classified, but otherwise I didn't review any classified documents.

Q So to the extent you talked about classified information, it was with a subject matter expert, but not reviewing any documents?

A Yes, that's correct.

Q Had you previously, unrelated to this litigation, reviewed classified versions of any of the documents that you reviewed in unclassified form?

A Yes.

Q Are you generally familiar with the classified portions of those documents?

A Yes, I am.

Q Did you meet with your counsel in preparing?

A I did.

Q You mentioned that you met with a subject matter expert. That's an NSA employee?

A Yes, it's an NSA employee.

Q What role does that individual have

within the NSA?

A An expert in upstream.

Q Is that the only subject matter expert within the NSA you met with?

A Yes, it is.

Q What's the general nature of what you talked about with that individual in unclassified form?

A We reviewed what was in the classified and in the unclassified to make sure we had a full understanding of how upstream worked and we were clear as to -- I was clear as to exactly where those lines, in terms of classification versus nonclassified information, could be discussed.

Q Okay. Was the primary purpose of that meeting to discuss that line between classified and unclassified information?

A It was more just to make sure that my memory from all of the work we had done over the last four years at NSA on upstream was current and understanding, and that I wasn't mixing and matching different activities.

So it was more of a verification that I knew exactly what it was, and this is what was classified and this wasn't.

Q Aside from preparing for this deposition, have you been involved in this litigation otherwise?

A No, I have not.

Q You've not reviewed any of the government submissions in this case?

MR. PATTON: Objection, vague as to time.

BY MR. ABDO:

Q You can answer the question.

A I reviewed all of the materials that have been provided, most everything in the binders. So, yes, I've read all of that material.

Q Did you review any documents before they were filed by the government in this case? Let me try that again.

Did you review any of the government submissions in this case prior to their being filed in court?

A I did not.
Q Have you been involved in any other litigation concerning Section 702 of the Foreign Intelligence Surveillance Act?
A No, I have not.
Q Are you familiar with other litigation concerning Section 702?
A I am.
Q What other litigation are you familiar with?
A There's at least one other lawsuit having to do -- that goes back quite a few years, sometimes referred to as the Jewel litigation.
Q Okay. So what's your current position at the NSA?
A I'm the Director of the Civil Liberties, Privacy, and Transparency Office.
Q How long have you been in that position?
A A little over four years.
Q What are your roles and responsibilities in that position?

A I set up the office four years ago, and I report directly to the Director of NSA. I'm an adviser on civil liberties, privacy, transparency issues to both the Director, as well as our Senior Leadership Team.

I review programs to identify civil liberties and privacy risks. I identify ways to mitigate them. I also work on transparency issues, publishing reports, meeting with civil society/non-governmental organizations, and then also act as the privacy advocate for NSA agency employees.

Q Are you responsible for that office's oversight of upstream surveillance?

A Could you clarify? I'm not sure what you mean by oversight of that.

Q Sure. Are you involved in your position in reviewing the operation of upstream surveillance as part of that office's mission?

MR. PATTON: Objection, vague.

You can answer.

THE WITNESS: My office reviews the

compliance incidents or other reports, oversight reports, as part of our role as information goes from NSA to ODNI.

BY MR. ABDO:

Q I just want to clarify that last portion. You said as part of your role, information goes from --

A ODNI. So -- sorry.

Our office is at a more strategic level, so we do not review every single compliance incident or every single activity specifically. We have a compliance group that does those types of functions.

My office is more strategic, so as specific reports or assessments are conducted either by ODNI or the Department of Justice, we're in that review process.

I'm also the main interlocutor with the Privacy and Civil Liberties Oversight Board, so to the extent that there are compliance incidences or changes to what -- any changes to how NSA is conducting its mission as it relates to

counterterrorism, we provide that type of information and those types of briefings to the PCLOB.

Q So in that role, you're not involved in the implementation of upstream surveillance?

MR. PATTON: Objection, vague.

THE WITNESS: So certainly at the -- there are decisions that are being made, we're informed, we will help decide, help with providing recommendations about whether it should go A or B or C, depending on specific questions that arise.

I'm not sure I'm answering your -- I'm not sure I'm fully understanding what you're trying to get at.

BY MR. ABDO:

Q Let me try to be clear.

When the government applies for authority from the Foreign Intelligence Surveillance Court to conduct upstream surveillance, is your office involved in that process?

A Yes.

Q And what's the nature of your office's involvement in that process?

A We review the minimum -- the proposed -- we will review any of the procedures. We will review any of the materials to ensure that we think that privacy has been properly protected, and civil liberties.

Q And that review happens prior to submission of an application to the Foreign Intelligence Surveillance Court?

MR. PATTON: Objection, vague.

You can answer.

THE WITNESS: Ask the question again.

BY MR. ABDO:

Q Sure. When the government is applying for authority to conduct surveillance under Section 702 of FISA -- are you familiar with the shorthand FISA for Foreign Intelligence Surveillance Act?

A I am.

MR. PATTON: Could I just interrupt?

I keep objecting to vague because

we're talking about 702, but there's PRISM and Upstream, and so if you want to be more specific, that's the nature of my objection.

MR. ABDO: That's helpful. Thanks, Rodney.

BY MR. ABDO:

Q When the government is applying for authority to conduct upstream surveillance from the Foreign Intelligence Surveillance Court, does your office review those applications prior to their submission to the Foreign Intelligence Surveillance Court?

A I understand. Hold on. Sorry, I'm looking for something specific to make sure I'm --

MR. PATTON: Take your time.

THE WITNESS: Can I talk -- take a break to make sure?

MR. PATTON: Sure.

BY MR. ABDO:

Q I just want to be clear. Just two quick things. Could you please first identify what you're looking at just for the record?

A I'm looking at the Objections and Responses by Defendant National Security Agency and Admiral Michael S. Rogers, Director, Plaintiffs' First and Second Sets of Requests for Admission.

Q And could you tell us whether you're looking to take a break to discuss classified versus unclassified information, or something else? Are you looking to discuss with your counsel the line between classified and unclassified information?

A Yes.

Q Okay. I think let me actually just withdraw that question. I don't think we need to take the time to go there.

MR. PATTON: Just to be clear to Mr. Abdo's point, the purpose of taking a break is not to talk about whatever the response is if it's not a subject of privilege.

The time to take a break and the need to take a break is related to whether to assert the privilege, and the nature and scope of the

privilege.

MR. ABDO: Thanks.

BY MR. ABDO:

Q You said that you had been in your current position for four and a half years?

A Yes.

Q Before that, were you also with the federal government?

A Yes.

Q And what position did you hold before your current one?

A I was the Senior Director for Privacy Compliance at the Department of Homeland Security in the Privacy Office.

Q How long were you in that position?

A Just shy of ten years.

Q And what were your roles and responsibilities there?

A I was in charge of developing the Privacy Impact Assessment process, publishing Privacy Act System of Records Notices, ensuring that the review of all IT systems within the

Department of Homeland Security had been reviewed for privacy considerations.

Q As part of that job, were you involved in any way in upstream surveillance?

A No.

Q As far as you know, did your roles or responsibilities in that job have any bearing on this lawsuit?

A No, not to the best of my knowledge.

Q Can you just briefly explain what a Privacy Impact Assessment is?

A Sure. It's a requirement of both the E-Government Act of 2002, as well as the Homeland Security Act, Section 222, which requires that the chief privacy officer ensure technology sustains and does not erode privacy.

It's the process by which the Department of Homeland Security and other federal agencies review technology to ensure they understand what the impact would be on privacy and how they might be able to mitigate it.

It's also a transparency document to

allow the public to know and understand what the agency is doing with their information.

Q And you were involved in the issuance of those sorts of assessments when you were at the Department of Homeland Security?

A Yes.

Q Prior to holding that position, were you also in the federal government?

A No. I worked for a small nonprofit called TRUSTe, which at the time was a nonprofit reviewing privacy policies and issuing seals of approval at the bottom of websites -- or generally seen at the bottom of websites, indicating that the privacy policy can be trusted.

Q How long were you in that position?

A I think about three years, maybe a little more, maybe a little less.

Q Were the two jobs within the federal government that you've discussed so far the only two jobs you've held in the federal government?

A No. Prior to working at TRUSTe, I worked at the Department of Commerce in the

e-commerce task force helping to negotiate the Safe Harbor Accord, which is the privacy agreement between the European Commission and the Department of Commerce for companies regulated by the Federal Trade Commission or the Department of Transportation to be able to transfer data from the EU to the US if they've agreed to a set of privacy policies.

Q What was your position then?

A I was the intern.

Q How long did you have that internship?

MR. PATTON: Don't knock it.

THE WITNESS: Don't knock it, man.

MR. ABDO: We all did.

THE WITNESS: I was there for a year. During that time frame, I went from being there called a co-op student, which means I was paid, to a full-time employee.

BY MR. ABDO:

Q But the full time you were there was one year?

A Yeah.

Q Okay. Is that the only other job you've had in the federal government?
A Yes.
Q Did that job in any way concern upstream surveillance?
A No. It was before upstream surveillance existed.
Q Can you describe your training in the areas of computer science, computer engineering, telecommunications networks, or network surveillance prior to joining the NSA?
A I do not have --
MR. PATTON: Object. Object to form, relevance.
MR. ABDO: You can answer.
MR. PATTON: You can answer.
THE WITNESS: Okay. I don't have any specific training on those four topics prior to being at NSA.
BY MR. ABDO:
Q Do you have any formal technical training from your -- let me try to be clear.

Do you have any training with respect to those four topics through, you know, college or any other graduate programs?

A No, I do not.

Q Do you have any familiarity with those topics from your time prior to joining the NSA?

MR. PATTON: Objection, vague.

THE WITNESS: Certainly my experience of working on Privacy Impact Assessments at the Department of Homeland Security, as well as working through different Internet activities, has given me a great deal of on-the-job experience.

I have no formal training to speak of in computer science or the other topics you've mentioned.

BY MR. ABDO:

Q Can you describe the on-the-job training you got in your position at the Department of Homeland Security on those four topics? And let me just be clear, on the topics of computer science, computer engineering, telecommunications networks, or network

surveillance.

A The first three are all part of the process by which we were having to review extensively the types of technology that DHS was putting forward and better understanding them to ensure we understood the privacy implications. So how did the computer systems work? Sort of how was the information being moved? Where was the information being moved?

I have no formal experience beyond my work at NSA on network surveillance.

Q For your time still at the Department of Homeland Security, would you consult with technologists to better understand how the conduct that you were reviewing might impact privacy?

A Absolutely.

Q Was that a frequent part of your job?

A Yes. We worked very closely with the chief information officer, the chief information security officer.

We also had external experts to the Department of Homeland Security who did have

experience in all of these different topics who would provide external expertise as part of the Federal Advisory Committee Act, or FACA.

All of those were available if we had questions to ensure that both we were fully understanding the privacy impact, that we had an appreciation of the information we needed to, and were getting those expertise from across -- wherever in DHS we needed.

Q You said that network surveillance was not a topic on which you received on-the-job training during your time at DHS?

A Correct.

Q Is that because there were no network surveillance programs that your office was called upon to review at your time at DHS?

MR. PATTON: Objection.

THE WITNESS: I need --

MR. PATTON: Just a second.

Objection. I'm not sure of the relevance of that particular question, but besides that, it is vague, ambiguous, but the witness can

answer.

THE WITNESS: We're now hitting into an area of classification that I would need to go and discuss any further conversation on this having to do with DHS activities.

BY MR. ABDO:

Q Let me take a step back then.

You said before that you hadn't received any on-the-job training with respect to network surveillance during your time at DHS.

That's correct, right?

A Maybe a better way would be if you could explain what you mean by "network surveillance," and then I can better answer that question.

Q Sure. I mean the use of computers to monitor communications over a telecommunications network.

A I think what I would like to do is revise what my answer is to say that, yes, I did have on-the-job training associated with that, and to go any further into that likely is classified.

Q Okay. I don't think we need to go further.

A Okay.

Q I just wanted to understand the nature of your technical training prior to your joining the NSA.

A Okay.

Q So now let's move to your time at the NSA. Can you describe in unclassified terms your on-the-job training with respect to those four areas, which again are computer science, computer engineering, telecommunications networks, or network surveillance?

MR. PATTON: Objection to the question to the extent it calls for source and methods of the NSA, operational details of Upstream, which are protected by the state secrets privilege and 50 U.S.C. § 3605(a), 50 U.S.C. § 3024(i)(1).

The witness can answer the question to the extent that it's unclassified.

MR. ABDO: And to be clear here, I'm asking just for unclassified information.

And, Rodney, can we agree on a short form of your invocation of the state secrets privilege and the other two statutory claims of protection?

MR. PATTON: I will work on that. We can maybe make a deal that you will shorten your record and I'll shorten mine.

But my concern with in unclassified terms is it may be very difficult for the witness to separate out when it's a broad question like that as opposed to a very specific question.

MR. ABDO: If instead of using the term "classified" we used the term "protected," would that be clearer?

MR. PATTON: For me I think it's just the tell me about everything nature of the question, which is very difficult for her to come up with what is classified and what is unclassified on the spot, whereas specific questions are much easier where she's -- you know, her job is to know where the line is, and she knows where the line is.

This is asking about her entire thing, so that's my concern.

BY MR. ABDO:

Q Ms. Richards, do you think you can answer my question without disclosing classified information?

A I can answer. I'm not sure it will give you what you're looking for, but ...

Q Why don't we start with what you can do.

A My answer is I have extensive ability to talk to and learn from anyone within NSA about how we do our job. To the extent that it means I'm interacting with people in all four of those categories, that's what I do.

Q Do you consider yourself to be well technically versed or conversant in those four areas?

MR. PATTON: Object to the form.

MR. ABDO: You can answer.

THE WITNESS: I do.

BY MR. ABDO:

Q I think that's fine.

As part of your job at NSA, have you ever been required to learn technical concepts relating to the programs you were reviewing that you felt unable to learn or understand?

MR. PATTON: Object to the form.

THE WITNESS: I don't understand your question, so help me.

BY MR. ABDO:

Q Sure, yeah. Your job at NSA involves reviewing NSA surveillance programs, correct?

A Correct.

MR. PATTON: Object to the form.

THE WITNESS: Correct.

BY MR. ABDO:

Q And as part of reviewing those programs, you mentioned that you talk with NSA employees about how those programs work; is that right?

A Yes.

Q When talking with those employees

about NSA surveillance programs, have you ever felt unable to comprehend technical detail that you were being explained?

MR. PATTON: Object to the form, vague. You can answer.

THE WITNESS: No, I have never felt like I couldn't understand what they were saying, or what the concepts that they were explaining to me. Is that what you're asking me?

BY MR. ABDO:

Q Yeah, that's what I'm asking you.

A Okay. No, I've never had -- they have all been able to fully explain it, both in concept and in fact.

Q Okay, great.

(Deposition Exhibit 42 was marked for identification.)

BY MR. ABDO:

Q Ms. Richards, you now have in front of you what's been marked as Exhibit 42.

Do you recognize Exhibit 42?

A Yes, I do.

Q What is it?

A It is Objections and Responses by Defendants National Security Agency and Admiral Michael F. Rogers, Director, to Plaintiff's Interrogatories.

Q Could you please turn to page 17 of Exhibit 42 and read to yourself the question identified on that page as Interrogatory No. 12?

A (Witness reviewing document.)

Q Have you had a chance, Ms. Richards, to read just the interrogatory, the question itself, No. 12 on page 17?

A I'm sorry. Yes, I have.

Q Could you turn to page 18 of the same document, Exhibit 42, and read the paragraph on that page identified as RESPONSE, which is the response to Interrogatory No. 12 provided by the NSA, and let me know when you're done.

A (Witness reviewing document.) Okay.

Q Did you have any role in drafting or reviewing the NSA's response to Interrogatory No. 12?

MR. PATTON: Object to the form, vague as to time.

THE WITNESS: No, I did not.

BY MR. ABDO:

Q You didn't draft the response?

A I did not draft the response.

Q Did you see this response prior to its having been filed in federal court -- sorry, prior to this having been sent to the Plaintiffs in this lawsuit?

A No.

Q Since this response was provided to Plaintiff, have you reviewed this response?

A Yes.

Q And do you understand this response?

A Yes.

Q To your understanding, does the term "Internet backbone" include high-speed, ultra-high bandwidth data transmission lines between the networks of major Internet service providers?

MR. PATTON: Objection, calls for expert testimony of a telecommunications computer

expert. You can answer.

THE WITNESS: Certainly that is one example of what might be included in the Internet backbone.

BY MR. ABDO:

Q When you say -- what do you mean by "might be"?

A Well, as is noted in the definition, and as is actually when it first comes up in the testimony to the PCLOB, Internet backbone is a -- sort of for want of a better word, there's not a specific term that everyone turns to and says that is the Internet backbone, but rather is a general description.

And so there are a number of things, as is described here, that could be included in the Internet backbone. It's not yes or no.

Q But your understanding is that the high-speed, ultra-high bandwidth data transmission lines between the networks of major Internet service providers are one such example?

A Those could be one such example.

Q And the Internet backbone also includes high-speed, ultra-high bandwidth data transmission lines within the networks of major Internet service providers?

MR. PATTON: Objection to form, calls for expert testimony. You can answer.

THE WITNESS: You're making a distinction between within versus --

BY MR. ABDO:

Q Between, that's right.

A So with -- you're --

Q Sorry. My first set of questions related to data transmission lines between the networks of major Internet service providers -- in other words, those connecting one major Internet service provider to another -- and now I'm asking about the high-speed, ultra-high bandwidth data transmission lines within any given major Internet service provider.

MR. PATTON: Objection, calls for expert testimony. You can answer.

THE WITNESS: It certainly may be. I

wouldn't say -- it could be an example.

BY MR. ABDO:

Q Can you give other examples of high-speed, high bandwidth data transmission lines that would be part of the Internet backbone?

MR. PATTON: Objection, calls for expert testimony. You can answer.

THE WITNESS: There's the terrestrial and undersea circuits are other examples.

BY MR. ABDO:

Q Could you describe just a little bit more what you mean by those?

MR. PATTON: Same objection.

THE WITNESS: So both with Internet backbone, as well as terrestrial and undersea circuits, NSA doesn't have a specific NSA definition. It's what would be generally accepted by a telecom expert. So there's nothing special about what those are.

BY MR. ABDO:

Q And I'm not asking for a special definition of Internet backbone. I'm asking

whether your understanding of that term would encompass the sort of data transmission lines we were just discussing.

MR. PATTON: Objection to form, vague, and calls for expert opinion.

THE WITNESS: So I guess my answer hasn't changed, and to go any further would put us into classified information.

And so to the extent that the information you have in the response -- there's no additional information that is -- I can switch words around, but in essence, those are different types of examples that could be part of what the Internet backbone is, but there's no additional information I can provide to you that's not classified.

BY MR. ABDO:

Q I understand that you may not be able to provide an unclassified response to this question, but could you state whether the NSA considers high-speed, ultra-high bandwidth data transmission lines between and within the networks

of major Internet service providers to be part of the Internet backbone for purposes of upstream surveillance?

MR. PATTON: Objection, asked and answered. Objection, calls for expert testimony. And also objection that it is calling for classified information and information protected by the previously mentioned statutes, so I'll instruct the witness not to answer that question.

BY MR. ABDO:

Q Are you going to follow your lawyer's instruction not to answer the question?

A Yes.

MR. ABDO: Rodney, can we agree that every time you instruct Ms. Richards not to answer a question on the basis of its classification, you will consider us to have noted our objection to it and we can move on?

MR. PATTON: Absolutely.

MR. ABDO: Okay.

MR. PATTON: I mean, there may be other ways to ask the question to get around that.

That's part of the problem.

MR. PADGETT: Maybe we should take a break because I think there is something that could be said, but the question is throwing it off.

MR. PATTON: Right, that's what I was just saying. There may be an answer to the question, depending on how it's phrased, that we could provide an unclassified response, and so we want to try and provide as much of an unclassified response as possible, but the way the question is framed leads us into a classified area.

MR. ABDO: Let me try to ask it one other way.

BY MR. ABDO:

Q Is your understanding that telecommunications networks experts would consider the high-speed, high-bandwidth data transmission lines between and within the networks of major Internet service providers to be part of the Internet backbone?

MR. PATTON: Just take a pause.

(Counsel conferring.)

MR. PATTON: Just object to the form in terms of calling for expert testimony, but you can answer that question.

Do you need the question read back?

MR. ABDO: We can do that if that's easier.

THE WITNESS: Yeah, can you read the question one more time? Sorry. Too many things.

(The reporter read back the question.)

THE WITNESS: I think generally speaking, yes.

MR. ABDO: Rodney, if you want to take a -- if there's more you think that can be provided after a short break, we're happy to do that now.

MR. PADGETT: It might be helpful.

MR. GILLIGAN: Actually, 30 seconds.

MR. ABDO: Go off the record.

(Off the record at 10:02 a.m.)

(Resume at 10:05 a.m.)

MR. PATTON: So we've clarified the

lines as to where the privileged information in that line of questioning is, so you can ask your next question, hopefully get a response.

BY MR. ABDO:

Q Sure. Is there a way that I could have asked the last set of questions I was asking in a way that you could answer with unclassified information?

A To the extent the term "Internet backbone" is what is generally understood, as amorphous as that definition is, by a telecommunications expert, that's how NSA would describe it.

To the extent you are connecting it in some way to upstream, that's where you get to classified information.

So they're sort of differentiating between those two, but NSA doesn't have a special definition.

Q Right. And I think you answered the question with respect to the term "Internet backbone" as understood by telecommunications

networks professionals or experts, but just to be clear, that term, as used by telecommunications networks experts, includes the high-speed, ultra-high bandwidth data transmission lines between and within the networks of major Internet service providers, right?

A Yes.

MR. PATTON: Objection to the extent it calls for an expert opinion.

THE WITNESS: But generally yes, that would be what I believe they would say, and so that would be what NSA would say.

BY MR. ABDO:

Q Okay. Going back to the NSA's response to Interrogatory 12, what does the term "data transmission lines" refer to?

MR. PATTON: Objection, calls for expert opinion.

THE WITNESS: Lines that transmit data. I mean, beyond what a tele- -- so I'm not a telecommunications expert, as we've noted. That doesn't mean I don't understand how they work, but

there's no special definition here that is distinct to what NSA does.

BY MR. ABDO:

Q What I'm getting at is does the term "data transmission lines" refer to the physical means of transmission of data, or something else?

MR. PATTON: Same objection.

THE WITNESS: I will go back to that it has no special particular meaning beyond what a telecommunications expert would expect.

BY MR. ABDO:

Q Is your understanding that a telecommunications network expert will use that term, "data transmission lines," to refer to a physical means of transmission, such as, for example, a cable or a wire or an optical fiber?

MR. PATTON: Object. Object to the form, vague, and calls for expert testimony.

You can answer.

THE WITNESS: As opposed to?

BY MR. ABDO:

Q As opposed to logical or virtual

groupings of data transmitted from one point to another.

MR. PATTON: Same objections.

BY MR. ABDO:

Q I'm really just trying to understand the term that you've used in your response to Interrogatory No. 12, and the term is "data transmission lines," and what I'm trying to understand is whether that refers to physical lines of transmitting data, or other ways of transmitting -- other ways of understanding the transmission of data.

A Oh, okay.

Q Do you understand that question and what I'm trying to understand?

A Do you want to go a little further? What would be the -- I guess I'm tripping over this seems to be logical on its face, and so I'm not sure -- I'm having a hard time -- it sort of defines itself, so ...

Q So in another interrogatory response, the NSA uses the term "virtual circuit." I'm

trying to understand whether this term, "data transmission lines," is limited to physical transmission lines or something else, like virtual circuits?

MR. PATTON: Object to the form, calls for expert testimony.

THE WITNESS: Do you want to point to where virtual circuits is so I can make sure I'm not tripping up or -- I do remember seeing virtual circuits, I just don't --

BY MR. ABDO:

Q Turn to page --

A I want to make sure I'm looking at the same one that you're looking at.

Q If you turn to page 6 of Exhibit 42, it's the response to Interrogatory No. 2, designated on that page by the all caps word RESPONSE.

Do you want to take a second to read those two paragraphs to yourself?

A Yeah. (Witness reviewing document.)

Oh, okay.

Q Having read that, do you now understand what I'm asking with respect to the term "data transmission lines"?

A Yeah, it's physical data transmission lines. There's nothing -- there's nothing virtual or -- there's nothing -- it's a physical transmission line.

Q Okay, okay. Would a fiberoptic cable qualify as a data transmission line as that term is understood by telecommunications network experts?

MR. PATTON: Objection, calls for testimony by a telecommunications expert.

You can answer.

THE WITNESS: Yes, it would. That would be one example. I'm not saying that's the only example, but it's certainly an example of what might be included in that.

BY MR. ABDO:

Q Okay. Would it also include -- let me phrase the question fully.

Would the term "data transmission

line" also include optical fibers within a fiberoptic cable as that term is used by telecommunications networks and network professionals?

MR. PATTON: Objection to the extent it calls for testimony by those telecommunications experts. You can answer.

THE WITNESS: To the extent that's an example of what might be included in that, yes.

BY MR. ABDO:

Q Would a fiberoptic cable be a data transmission line as that term is understood by the NSA?

MR. PATTON: Same objection.

THE WITNESS: Can you repeat the question? I'm not sure I understood.

BY MR. ABDO:

Q Sure. Does the term "data transmission line," as the NSA has used it in response to Interrogatory 12, include fiberoptic cables?

MR. PATTON: Objection to the extent

it calls for expert testimony. You can answer.

THE WITNESS: Yes.

BY MR. ABDO:

Q Okay. And the same is true of --

A It's an example. I mean, all of these are examples. NSA doesn't have a special definition for "Internet backbone" or these other well-known telecom-like words that you're bringing up, data transmission line or fiberoptic line.

Q Does the term "data transmission line," again as used in the response to Interrogatory 12, include individual wavelengths of light carried over fiberoptic cables?

MR. PATTON: Object to the form to the extent it calls for expert testimony.

You can answer.

THE WITNESS: Certainly it is an example.

BY MR. ABDO:

Q Would the term include any subdivisions of a wavelength of light carried over a fiberoptic cable?

MR. PATTON: Same objections.

You can answer.

THE WITNESS: Would the subdivision of the light?

BY MR. ABDO:

Q Would any subdivisions of a wavelength of light carried over a fiberoptic cable constitute a data transmission line as the NSA has used that term in responding to Interrogatory 12?

MR. PATTON: Objection to the extent it calls for expert testimony. You can answer.

THE WITNESS: So to the extent that any of those are an example of what might be part of the Internet backbone, in which case it's providing high-speed, ultra-high bandwidth data transmission lines, the answer would be yes.

MR. ABDO: Okay. Do you mind if we take a five-minute break to use the restroom?

MR. PATTON: No.

(A break was taken at 10:15 a.m.)

(Resume at 10:25 a.m.)

BY MR. ABDO:

Q Ms. Richards, where do you acquire your understanding of the term "Internet backbone"?

A From both experts within NSA, as well as talking to -- or actually reading what's, you know, sort of been written on it in telecommunications just sort of generally.

Q Did you talk to anyone at the NSA about the meaning of the term "Internet backbone" in preparing for this deposition?

MR. PATTON: Objection to the question to the extent it calls for attorney-client privilege or any classified information, but you can answer to the extent that it is not attorney-client privileged.

THE WITNESS: Certainly in preparation for this we reviewed the definitions that have been provided to ensure that I understood them and that nothing had changed.

BY MR. ABDO:

Q Did you talk with any subject matter

experts at the NSA about the meaning of the term "Internet backbone"?

A Yes, I did.

Q Did you talk to them about anything beyond what was provided by the NSA in response to Interrogatory 12 asking for the definition of "Internet backbone"?

MR. PATTON: Object to the form, vague.

THE WITNESS: We discussed the definition and understood it to be the same as the definition that a subject matter expert in the telecommunications industry would use.

I'm not sure I'm understanding or answering what you're asking me.

BY MR. ABDO:

Q Did you talk about the terms used in the definition provided of the term "Internet backbone"?

A Yes.

Q You understand that the definition of the term "Internet backbone" is one of the terms

listed in topic 2 of the deposition notice of the case?

A Yes.

Q And you understand that the NSA has an obligation under the federal rules to provide somebody for this deposition who knows the Agency's understanding of that term?

A Yes.

MR. PATTON: Object to the extent it calls for a legal conclusion.

Just wait for my objection --

THE WITNESS: Sorry.

MR. PATTON: -- or non-objection.

BY MR. ABDO:

Q So you understand what I'm asking about? When I'm asking about the NSA's understanding of certain terms, I'm asking for the NSA's understanding, as you're a designee of the NSA today.

A Yes.

Q Okay. I want to move to a different term used in your definition.

The definition or use of the term "large, strategically interconnected computer network," what does that term mean?

MR. PATTON: Objection to the extent it calls for expert testimony. You can answer.

THE WITNESS: The words have no specific meaning beyond what you would expect from a telecommunications expert.

They're large, they're strategically connected, and they're computer networks. Perhaps when we --

BY MR. ABDO:

Q Is that the -- well, let me ask by example. Would that term, "large, strategically interconnected computer networks," include the networks of major Internet service providers inside the United States?

MR. PATTON: Objection to the extent it calls for expert testimony. You can answer.

THE WITNESS: To the extent that that might be one example of what would be included in the Internet backbone, yes, that's an example.

BY MR. ABDO:

Q I'm not sure I understood the first part of your response. Is it or is it not -- sorry, let me start that over.

Would or would not a network of a major Internet service provider constitute a large, strategically interconnected computer network as the NSA has used that term?

MR. PATTON: Object to the form to the extent it calls for expert testimony.

You can answer.

THE WITNESS: Let me clarify what I think you're asking to make sure I understand.

You're saying would a large -- I'm sorry, a communications provider in the United States be considered a strategically interconnected computer network?

BY MR. ABDO:

Q Yes.

A Yes.

Q Okay. Approximately how many data transmission lines are there that satisfy the

definition of "Internet backbone" given by the NSA?

MR. PATTON: Object to the form to the extent it calls for expert testimony.

You can answer.

THE WITNESS: If you go back and look at -- I believe it's the request for admission.

BY MR. ABDO:

Q You're welcome to refresh your recollection using that document, but I'd like your answer to that question.

A Okay, so could you ask your question one more time?

Q Sure. Approximately how many data transmission lines are there that satisfy the definition of "Internet backbone" given by the NSA?

MR. PATTON: Objection to the extent it calls for expert testimony.

THE WITNESS: How many data transmission lines meet the definition -- I'm sorry?

BY MR. ABDO:

Q Yeah, sorry, let me say it one more time. Approximately how many data transmission lines are there that satisfy the definition of "Internet backbone" given by the NSA?

MR. PATTON: Just object, first again to the extent it calls for expert testimony, and second, to the extent it is beyond the 30(b)(6) deposition notice.

Just to be clear, to the extent it's beyond the deposition notice, she'll be answering in her personal capacity as opposed to her capacity as a 30(b)(6) NSA designee.

I'll shorten that next time.

MR. ABDO: Just for the record, would you let us know what you're looking at?

THE WITNESS: I am looking at the Request for Admission response -- Request for Admission No. 1 and No. 2, just to try and make sure I'm -- I don't think that this -- how many data transmission lines are there that satisfy the definition.

MR. PATTON: The definition is Interrogatory Response 12; is that right?

THE WITNESS: Correct.

BY MR. ABDO:

Q If you don't know the answer, you don't know the answer. I'm asking whether you know the answer.

A I don't know the answer. I'm sorry.

Q Is there anyone at the NSA who would know the answer to that question?

A So to the extent that the answer to that question is available to the public -- so I guess to the extent that that information may be available in the public, we didn't -- I don't know, I mean, actually.

Q Do you know whether anyone at the NSA would know the answer to that question even if based on information not available to the public?

MR. PATTON: Well, object.

THE WITNESS: So I think --

MR. PATTON: Object to the form to the extent it calls for classified and otherwise

protected information.

The witness can answer the question if she's confident that the answer is unclassified. I'm not. I am not.

THE WITNESS: The answer to your question, to the extent it's unclassified, and to the extent it is known, would be in the public sphere and not something specific to NSA's -- to how NSA functions or what NSA does.

BY MR. ABDO:

Q Just so I understand it, is your response then that there's a further answer you could give, but will refuse to on the basis of its classification?

In other words, is there more you would say but for your belief that answering my question would disclose classified information or protected information?

MR. PATTON: Objection. The answer I believe calls for classified information and information otherwise protected by the statutory privileges, and I instruct the witness not to

answer.

BY MR. ABDO:

Q Are you going to follow your --

A I am going to follow my lawyer's --

Q -- instruction not to answer?

A -- instruction not to answer.

Q Is your understanding then that even answering my question of whether providing an answer to my question would disclose classified information is itself classified?

MR. PATTON: Same objection.

Just a second.

(Counsel conferring.)

THE WITNESS: I think it would --

MR. PATTON: Just a second.

MR. PADGETT: Could you read back the question?

THE WITNESS: I just wanted to read back the question, yeah, or you can restate the question.

BY MR. ABDO:

Q Let me restate the question. I'll go

back to what I think started us down this path.

I originally asked whether there's somebody at the NSA who knows how many data transmission lines there are that satisfy the definition of "Internet backbone" provided by the NSA. I believe you said you don't know the answer, so I asked whether somebody at the NSA would know the answer to that question.

Then I believe you said, please correct me if I'm wrong, that to the extent there's an answer that you can provide publicly to that question, it was provided in the NSA's responses to our requests for admission.

A Can we go out on a classified -- could we take a --

Q Sure.

MR. PATTON: Yes. I just want to say before we go off the record that object to the extent it misstates the prior testimony, and that she also said that it doesn't mean anything different in an unclassified sense than what telecommunications experts would say.

BY MR. ABDO:

Q Okay. You understand that I was asking about knowledge that the NSA has irrespective of whether that information is available to the general public.

A I did understand. What I said was I was not answering about what NSA knew or didn't know because there's a classification issue, but to the extent there was an answer to your question, it would be whatever you could find in the public.

And so similar to what you see in response to RFA 1, where we give the information that TeleGeography publishes, to the extent they have information that would say -- provide the answer to this question, but I don't think that the answer to RFA 1 was the same as what you were asking.

MR. PATTON: And so we'll go off the record and see if there's more information that can be provided unclassified.

MR. ABDO: That's fine, although I'm

also trying to establish whether there's somebody at the NSA who would be able to provide a classified response, even if not here today, whether there's somebody who could provide that response if we were to move to compel that response.

It sounds as though you're not that person from what you're saying. I'm trying to understand if there's somebody else who is that person.

THE WITNESS: And so could we please --

MR. PATTON: Wait a second.

And we're trying to figure out whether we can tell you that.

THE WITNESS: Yes, so let us go have that --

MR. ABDO: We'll go off the record for a few minutes.

(Off the record at 10:38 a.m.)

(Resume at 10:47 a.m.)

MR. PATTON: Have we got a question

pending?

MR. ABDO: Yes, we have a question pending, and as I understand it, Ms. Richards, you went out to consult with counsel about whether you could respond to my question without disclosing classified information.

Have you arrived at a conclusion?

MR. PATTON: Yes. It's like a jury, we have arrived at a verdict.

So just to put my objections on the record, one is that it calls for expert testimony; two, it is beyond the 30(b)(6) notice, and therefore the witness's answer, if she were to give one, would be in her personal capacity as opposed to her capacity as a 30(b)(6) witness.

And if I understand the question correctly, anything beyond the unclassified information that's already been provided in the RFA, we can neither confirm nor deny whether or not --

MR. PADGETT: I'm sorry.

(Counsel conferring.)

MR. PATTON: So striking the last part, whether NSA has any nonpublic information going beyond what's already in the RFA we can neither confirm nor deny, so on that basis, instruct the witness not to answer the pending question.

BY MR. ABDO:

Q And you'll follow your lawyer's instruction not to answer?

A I will follow my lawyer's advice not to answer.

Q Okay. Could you please turn to page 5 of Exhibit 42 -- sorry, page 6 of Exhibit 42. You were here a moment ago, but if you need to, would you please re-read the two paragraphs designated as "RESPONSE" on that page.

A I'm sorry, to clarify, we're on the interrogatories?

Q Yes. Exhibit 42 are the NSA's Responses and Objections to Plaintiff's First Set of Interrogatories, page 6.

A Page 6, yes.

Q If you need to, just refresh your memory of that response.

A Yes.

Q Is an international submarine cable that connects two stations a circuit as the NSA has defined that term in response to Interrogatory No. 2?

MR. PATTON: Objection to the extent it calls for expert testimony.

THE WITNESS: As with Internet backbone, "circuit" has no specific NSA meaning. It is the meaning that a telecommunications expert would expect it to mean. There's nothing something special. So I just want to make sure that that's clear, there's not some other definition out there.

To the extent that you asked whether two submarine cables would be -- I'm sorry, I just want to make sure.

BY MR. ABDO:

Q Whether an international submarine cable that connects two stations is a circuit.

A Yeah.
MR. PATTON: Same objection.
THE WITNESS: Yes.
BY MR. ABDO:
Q Okay. Is an international submarine cable that connects two stations a circuit on the Internet backbone?
MR. PATTON: Object to the form, vague. Objection to the extent it calls for expert testimony.
THE WITNESS: Say it one more time.
BY MR. ABDO:
Q Do you want me to repeat that?
A Yes, please.
Q Sure. Is an international submarine cable that connects two stations a circuit on the Internet backbone?
MR. PATTON: Objection to the extent it calls for expert testimony.
THE WITNESS: Yes.
BY MR. ABDO:
Q Okay. Is each optical fiber within an

international submarine cable that connects two stations a circuit?

MR. PATTON: Objection. Same objection as before.

THE WITNESS: Each of these is an example of what might be a circuit and what might be considered the Internet backbone.

So to the extent an optical fiber is given as an example of a circuit, then the answer would be yes, but they're an example.

BY MR. ABDO:

Q That's right. I'm not asking -- let me try to be clear.

A Okay.

Q Each of these questions is asking whether a particular data transmission line connecting two stations constitutes a circuit. I'm not asking for you to confirm that that's the only sort of circuit out there.

A Okay.

Q So I am asking whether these are examples of a circuit, not whether they are the

sum total of what might be a circuit.

A Okay.

Q With that understanding, is your answer to my last question -- what is your answer to my last question, which was is each optical fiber within an international submarine cable that connect two stations a circuit?

MR. PATTON: Objection to the extent it mischaracterizes the prior testimony. Objection, calls for expert testimony.

THE WITNESS: Circuit could -- the definition of "circuit" being two stations, instruments transmitting information, could be an example of -- could be an example. So it could be, yes.

BY MR. ABDO:

Q When you say it could be, you're referring again to an optical fiber within an international submarine cable?

A Yes, it could be.

Q If an optical fiber within an international submarine cable has been

multiplexed, would each of the subdivisions created by that multiplexing be a circuit?

MR. PATTON: Objection to the extent it calls for expert testimony. You can answer.

THE WITNESS: It could be.

BY MR. ABDO:

Q In what circumstance would it be, and in what circumstance would it not be?

A I'm trying to think if there's an example where it wouldn't be. I think the definition --

MR. PATTON: Same objection to that question and this line of questioning.

THE WITNESS: Yeah. So a telecommunications expert would undoubtedly consider it to be a circuit.

BY MR. ABDO:

Q Would the NSA also consider it to be a circuit?

A To the extent that there's no --

MR. PATTON: Object. Objection to the form to the extent it calls for expert testimony.

THE WITNESS: To the extent that there's no difference in the definition that NSA takes versus what a telecommunications expert takes, there's no special meaning to the word "circuit." So if they would consider it to be a circuit, then NSA would consider it to be a circuit.

BY MR. ABDO:

Q Okay. Can a single circuit span multiple physical paths between two stations?

MR. PATTON: Objection, vague. Objection, calls for expert testimony.

THE WITNESS: Can a single --

BY MR. ABDO:

Q Can a single circuit span multiple physical paths between two stations?

And I understand you'll make the same objections.

MR. PATTON: Same objections. And I would just add beyond the scope of 30(b)(6), and therefore the witness will be testifying in her personal capacity as opposed to her 30(b)(6)

designee capacity.

MR. ABDO: Rodney, if it's okay with you, can we shorten that objection to it's beyond the scope?

MR. PATTON: As long as you understand that what that means here is that she's testifying as Becky Richards and not testifying as a 30(b)(6) witness for the NSA.

MR. ABDO: Thanks. I will so understand it.

THE WITNESS: And I will --

BY MR. ABDO:

Q Let me restate the question.

A I've now lost what the question is as Becky answering.

Q Let me restate it, okay?

Can a single circuit span multiple physical paths between two stations?

MR. PATTON: Objection, calls for expert testimony. Objection, beyond the scope of 30(b)(6).

THE WITNESS: I'm going to answer I

don't know.

BY MR. ABDO:

Q Do you know whether there's anybody else at the NSA who would know the answer to that question?

MR. PATTON: You can answer if you have an unclassified --

THE WITNESS: I don't know.

BY MR. ABDO:

Q You don't know whether there's somebody else at the NSA who would know the answer to that question?

A Correct.

Q Did you talk to any subject matter experts at the NSA about the meaning of the term "circuit" prior to this deposition?

A I did.

Q As part of that conversation, did you do anything beyond reviewing the definition of "circuit" provided by the NSA in response to our Interrogatory No. 2?

MR. PATTON: Objection, vague.

THE WITNESS: We discussed generally what is meant by "circuit" in the context of a telecommunications expert.

We did not get to the specific whatever you just asked of a single circuit having multiple physical paths.

BY MR. ABDO:

Q Okay. What's your understanding of the term "virtual circuit"?

MR. PATTON: Object to the form, calls for expert testimony, and beyond the scope of 30(b)(6).

THE WITNESS: As described in the -- are we still on the interrogatories on page 6 in response to No. 2?

BY MR. ABDO:

Q Yes. Let me try to be clear.

What is your understanding of the term "virtual circuit" as used by the NSA in its response to Interrogatory No. 2?

A My understanding is that there's a way in which to use different techniques to divide the

circuits so that you have more than one -- multiple circuits on one circuit.

Q Let me just try to understand that. Do virtual circuits -- let me start over. Can a virtual circuit traverse multiple physical circuits?

MR. PATTON: Objection to the extent it calls for expert testimony, and beyond the scope of 30(b)(6).

THE WITNESS: I'll respond I don't know.

BY MR. ABDO:

Q Is there anyone at the NSA who would know the answer to that question?

A I don't know.

Q Did you talk with any subject matter experts at the NSA about the definition of or the meaning of the term "virtual circuit" as used in the NSA's response to Interrogatory No. 2?

A I did.

Q Is there anything about the meaning of the term "virtual circuit" that you can provide

beyond what is in the NSA's response to Interrogatory No. 2?

A Since I'm not the telecommunications subject matter expert, my answer is confined to what you see on the piece of paper.

Q Is there a telecommunications subject matter expert at the NSA who could more fully answer that question?

Let me restate the question.

Is there anyone at the NSA who could more fully define what the term "virtual circuit" means as used by the NSA in response to Interrogatory No. 2?

MR. PATTON: To the extent that the answer is yes or no, she can answer, but I'll note for the record that she's testified multiple times that the NSA does not mean anything different by the term "virtual circuit" other than what is understood within the telecommunications industry.

BY MR. ABDO:

Q What is the meaning of "virtual circuit" as understood within the

telecommunications industry?

MR. PATTON: I'm going to object to the question to the extent it calls for expert testimony, and beyond the scope of 30(b)(6).

BY MR. ABDO:

Q You can answer.

A I don't have anything further to define for you.

Q Is there anyone at the NSA who better understands the definition of "virtual circuit" as used by those in the telecommunications industry?

MR. PATTON: You can answer the question if it's unclassified.

THE WITNESS: I don't know.

MR. PATTON: You can't provide a name.

THE WITNESS: I don't know.

BY MR. ABDO:

Q You don't know whether there's anyone at the NSA?

A Correct.

Q It's true -- well, let me ask you.

Is it true that each Internet protocol

packet sent on the Internet is routed to its destination independently?

MR. PATTON: Object to the form of the question to the extent it calls for expert testimony, and outside the scope of 30(b)(6).

You can answer.

THE WITNESS: I'm sorry, can you ask the question again?

BY MR. ABDO:

Q Sure. Is it true that each Internet protocol packet sent on the Internet is routed to its destination independently?

MR. PATTON: Same objections.

THE WITNESS: Generally speaking, yes, that is my understanding.

BY MR. ABDO:

Q Are there circumstances you can think of where Internet protocol packets would not be routed independently on the Internet?

MR. PATTON: Object to the form to the extent it calls for expert testimony, and beyond the scope of 30(b)(6). You can answer.

THE WITNESS: Not off the top of my head, but I'm sure there are examples.

BY MR. ABDO:

Q Why are you sure there are examples?

A Just because every rule seems to have some sort of exception to it, so to say something is hard and fast to be always the case is not something I would like to do.

Q Okay. When Internet packets that constitute a single communication take different paths to a common destination, are those packets traversing different circuits or the same circuit?

MR. PATTON: Object to the form, lacks foundation, object to the vagueness of the term "single communication." Object that it calls for expert testimony, and it is beyond the scope of 30(b)(6). You can answer.

THE WITNESS: The question was if packets take a different path, are they on different circuits?

BY MR. ABDO:

Q Yes.

A I would say it depends. There's not, again, a hard and fast rule. Depending, it might be on the same circuit, it might be on a different circuit.

Q What does it depend on?

MR. PATTON: Same set of objections.

THE WITNESS: I guess it would depend on how -- what would it depend on?

It would depend on the nature of the circuit.

BY MR. ABDO:

Q What do you mean by the nature of the circuit?

MR. PATTON: Same objections.

THE WITNESS: Depending on how the packets were going and how you -- how is it routed? Do they take different paths, or are they on the same circuit?

So to the extent the circuit can be meant in a big sense or in a small sense, it's going to decide whether it's on the same circuit or not.

So you asked in a separate set of line, had a whole bunch of distinctions as to what was data transmission line and what were they, and was it a wavelength, or something further into that. So it will depend on how you define "circuit," which is why you were asking me to define "circuit."

BY MR. ABDO:

Q Let me just try to understand.

Does the answer to my question depend on whether the separate paths being taken by packets are being routed over one physical circuit or not?

MR. PATTON: Same set of objections.

THE WITNESS: One physical circuit?

BY MR. ABDO:

Q Suppose two packets that are part of the same communication traverse different optical fibers.

A Okay. Are those different circuits?

Q Yes, that's my question.

MR. PATTON: Object to the extent it

calls for expert testimony in a hypothetical, and also beyond the scope of 30(b)(6).

THE WITNESS: So --

MR. PATTON: Also asked and answered.

THE WITNESS: So if it's on two different circuits, then it's on two different circuits. I feel like I'm having a circular conversation, so I'm not sure. Can two packets be on the same circuit and take different paths?

MR. PATTON: I don't think that's the question.

THE WITNESS: Is that --

BY MR. ABDO:

Q My original question was whether packets that are traversing different paths to their common destination are traversing different circuits. And I believe, please correct me if I'm wrong, you said, generally, yes.

MR. PATTON: That's a misstatement of her prior testimony.

BY MR. ABDO:

Q Could you please tell us what your

answer is to that original question?

MR. PATTON: Do you want the question to be read back?

MR. ABDO: No. I mean, let's move on.

Would you mind, Ms. Jaques, marking this as Exhibit 43?

(Deposition Exhibit 43 was marked for identification.)

BY MR. ABDO:

Q So you have in front of you what's been marked as Exhibit 43.

Do you recognize that document?

A Absolutely.

Q And what is Exhibit 43?

A Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, July 2nd, 2014.

Q What was the NSA's relationship to the drafting or review of the report marked Exhibit 43?

MR. PATTON: Objection as vague, and

objection to the extent it may call for deliberative process privilege that might be invoked by the PCLOB that we don't represent. So maybe if you could ask a more narrow question, we can avoid most of the deliberative process.

She can speak in general terms on that, that would be good, in answer to your question, but I don't want to too broadly object on deliberative process grounds to protect PCLOB's privilege.

BY MR. ABDO:

Q Let me ask a different related question. Was the NSA involved in the drafting of Exhibit 43?

MR. PATTON: Objection, vague.

THE WITNESS: NSA provided expert testimony to the Board as is described on page 4 of the report. We provided documentation, we provided presentations, and we answered questions throughout their process.

We then for the fact section reviewed -- we reviewed the document for factual

accuracy, as well as we reviewed the entire document for classification to ensure there was no classified material in it.

BY MR. ABDO:

Q So I believe that you said that the NSA provided testimony, documentation, and presentations to the members of the PCLOB in drafting Exhibit 43, right?

A That is correct.

Q Do you know how many sessions the NSA provided testimony about the subject matter of the report that's marked Exhibit 43?

A It was a handful. I don't remember the exact number, but certainly they came to NSA, and we went to the PCLOB a number of times, both ways. We had conference calls, and we had email exchanges.

Q And did that testimony involve both classified and unclassified information?

A Yes, it did.

Q Is the same true of the documentation that the NSA provided to the PCLOB?

A Yes, it was both classified and unclassified.

Q And is that also true of the presentations provided?

A Yes, all was classified and unclassified.

Q And you say that the NSA reviewed the factual section of the report marked Exhibit 43 for accuracy; is that correct?

A That is correct.

Q When you say "fact section," what specific pages are you referring to, or page range are you referring to?

A Page 16 to 79. In essence, Part 3, Description and History.

Q Did the NSA review any other portion of the report marked Exhibit 43 for factual accuracy?

MR. PATTON: Objection to the form, vague as to time.

THE WITNESS: NSA otherwise did a classification review of the document.

To the extent these documents have the opinions of the various board members, NSA was not reviewing that information beyond ensuring there was no classified material in it.

BY MR. ABDO:

Q If the NSA, during its classification review of the portions of the report, other than Part 3, noticed a factual inaccuracy, would the NSA have notified the PCLOB of that inaccuracy?

A NSA conducted a classification review of the document. As part of that classification review, to the extent that something would be described in some of the other pieces of the document that was not not, we would notify them as part of that, as is noted again on page 4.

Q Let me just make sure I understand.

A Yeah.

Q The NSA reviewed Part 3 of the report marked Exhibit 43 for accuracy, right?

A That is correct.

Q It reviewed the entire document for classification, right?

A Correct.

Q And if in the process of reviewing the entire document for classification it noticed an inaccuracy outside the portion that it reviewed solely for accuracy -- sorry, outside the portion that it reviewed when it was conducting its review for accuracy, your testimony is that the NSA would have notified the PCLOB of that inaccuracy?

A Correct.

Q Was the NSA's review for accuracy of the factual section of the report thorough?

MR. PATTON: Objection, vague.

THE WITNESS: Yes.

BY MR. ABDO:

Q The NSA would have reviewed every sentence?

A Absolutely.

Q And what would the NSA have done if it noticed an inaccuracy in any portion of the report?

MR. PATTON: Objection, vague.

THE WITNESS: NSA would provide a

response explaining either why it was inaccurate or why the information in the classification review was classified, and there was -- as is important to remember in the Upstream, large portions of that program remain classified, and so necessarily with this report, with this NSA Civil Liberties and Privacy Office Report, the information is incomplete.

And so a lot of the conversation was a mixture of how do you provide an accurate representation of how Upstream works while keeping the sources and methods classified? And so a lot of the conversation, particularly around the accuracy and the classification, were tied together because of those reasons.

And so this gives, as does our report, and continues to, a broad accurate description of the outline of how the program runs, but does not get into some of the much more specific aspects to it.

BY MR. ABDO:

Q In the course of the review for

accuracy of the report, did the NSA notice inaccuracies and make recommendations to the PCLOB about how to fix those inaccuracies in what's now marked Exhibit 43?

A Yes.

Q Are you aware -- sorry, strike that.

Did the PCLOB generally accept those recommendations?

MR. PATTON: Just a second.

(Counsel conferring.)

MR. PATTON: Could you read the question back?

(The reporter read back the question.)

MR. PATTON: Just object to beyond the scope of the 30(b)(6).

And if the answer to that question is yes or no, you can answer. If the answer to that question is going to be a narrative description of what the PCLOB did or did not accept, then we're concerned that we might be in the deliberative process.

MR. ABDO: I just want to state for

the record, Rodney, you don't represent the PCLOB, correct?

MR. PATTON: I do not, but I am with the Department of Justice, and we do represent the United States, so here we would be preserving their ability to later assert that privilege if need be. I certainly am not in a capacity to waive it on their behalf.

MR. ABDO: I'm just not sure you're in a position to assert it though. I'm not sure we're asking for anything that's going to reveal the deliberations anyway, but I note that we object to your quasi-invocation of the PCLOB's deliberative process.

MR. PATTON: I can rephrase it as a preservation of their right to assert the deliberative process privilege, since they are not here to invoke that themselves.

MR. GILLIGAN: I would add that our function as Department of Justice attorneys is to represent the interests of the United States in this proceeding, and PCLOB is an independent

establishment of the United States government, but I understand your objection.

MR. ABDO: Sure, but you also know that we had -- you know, Topic 6 very clearly included this report as a subject of this deposition.

MR. PATTON: I doubt, again, that you will be delving into the details of that. There's an awful lot --

MR. GILLIGAN: The facts, not recommendations.

MR. PATTON: There's an awful lot of questions that the witness is perfectly capable of answering, so I don't think we're going to be in any --

BY MR. ABDO:

Q Ms. Richards, can you answer the question?

A Yes, I'll answer the question.

What I would do is point you to, again, page 4 that specifically says that they considered the Intelligence Community's comments

regarding the operation of the program to ensure accuracy. None of the changes resulting from that process affected the Board's substantive analysis and recommendations.

So I would point you to that to avoid this whole conversation about what is or isn't sort of privileged between it to say that they accepted our changes, they didn't change substantively what they were doing. We went through a back-and-forth to ensure that everybody understood how the program worked, what was classified.

In some instances, they asked for information to be declassified in order to make the record full, and that didn't change. So we went through that process.

Q Let me ask my question again because I don't think that answered it.

A Sure, okay.

Q If the NSA identified an inaccuracy in the report marked as Exhibit 43 to the PCLOB, would the PCLOB generally fix that factual

inaccuracy, generally have fixed it?

MR. PATTON: Object to the form, vague.

THE WITNESS: Yes. The PCLOB was not interested in having an inaccurate description of how Section 702 -- it was not within -- they didn't want to have that, and so they worked closely with us to ensure that they -- I don't know if "closely" is the right word, but they worked with us extensively in order to ensure that they had an accurate representation that could be made unclassified, which was -- up until -- there had -- the record had been not as extensive.

BY MR. ABDO:

Q Okay. Are you aware of any inaccuracies, factual inaccuracies, in the report marked as Exhibit 43?

MR. PATTON: Object to form, vague.

THE WITNESS: If there's particular sentences you would like me to look at or there's particular questions that you have, I'd be happy to look at those and walk through.

As a general matter, the information in here is accurate as a description, but necessarily, as I mentioned before, not a full description of the program because many of those facts still remain unclassified. But if there's particular sentences that you would like to point me to, I'm happy to review.

I would also note that, as of 2017, NSA changed one of the ways it was doing its collection, so it was no longer getting "abouts" collection. And so to the extent the material in here accurately reflects what was happening in 2014, the general matter, there may be, you know, slight, slight differences, but this is true.

That information has changed, so we are no longer doing a collection that gets the, quote, "abouts" collection in upstream. So to the extent that that's no longer accurate, that would be the case.

BY MR. ABDO:

Q But at least as the NSA was conducting upstream surveillance as of July 2nd, 2014, which

is the date of that report, you're not aware of inaccuracies in the report?

A Again, I would ask --

MR. PATTON: Sorry, just object to asked and answered. Go ahead, you can answer.

THE WITNESS: Again, if there are specific sentences you would like me to go to that you think maybe are not accurate, I'm happy to talk about those particular sentences. It's a 191-page document.

As a general matter, NSA considers this to be an accurate outline of the unclassified portions of Upstream. There may be particular sentences as they describe them, but the facts we believe to be accurate.

BY MR. ABDO:

Q Okay. I want to turn your attention to page 36 of the report marked Exhibit 43. Could you please read the first sentence of the very last paragraph that starts on that page? It begins "once tasked." Again, that's at the bottom of page 36 of Exhibit 43, and that sentence ends

on the next page, 37.

A Okay, yes.

Q Is that sentence factually accurate?

MR. PATTON: Object to the form, vague.

BY MR. ABDO:

Q As of the time -- let me start over.

Is the sentence that I just asked you to read at the bottom of page 36, carrying over onto page 37 of Exhibit 43, an accurate description of how upstream surveillance operated as of July 2nd, 2014?

A Well, what I would do is I would point you, rather than to the sentence that's on page 36 of the PCLOB report, and instead suggest that the RFA, Request for Admission, on page 9, in response to RFA for No. 8, that describes how this is -- how the government describes it.

The other place I would suggest, which is the government's description, is also in the NSA Civil Liberties and Privacy Office Report at page 5.

Those are both more accurate descriptions of how we would talk about Upstream. The description on page 36 is necessarily vague.

Q What's inaccurate about the sentence at the bottom of page 36, carrying over onto page 37, in Exhibit 43?

MR. PATTON: Objection, mischaracterizes prior testimony. And just a second, there might be a classified response.

We will need to find out what her answer is going to be on this to determine whether the answer is partially classified, fully classified, or wholly unclassified. At this point, I don't know what her answer is going to be.

MS. HANLEY COOK: Why don't we take a five-minute break.

MR. ABDO: Go off the record, Dawn, please.

(Off the record at 11:30 a.m.)

(Resume at 11:56 a.m.)

MR. ABDO: Ms. Jaques, do you mind

reading back the last question before we broke?

(The reporter read back the question.)

MR. PATTON: Objection to the extent it misstates prior testimony, and objection to the extent that the answer calls for classified information and information subject to the statutory privileges.

You can answer to the extent your answer is unclassified.

THE WITNESS: Okay. So this sentence, as I mentioned about the entire document and the sort of public description of Upstream, is necessarily incomplete because of the classification of information.

This sentence is accurate as of 2014, but I would point you to the description that's provided in the RFA, Request for Admission No. 8, in the response. That provides an accurate description of how upstream Internet collection works today, with, again, the understanding that it's necessarily incomplete.

To provide you a description of what

is different between those two and why necessarily gets into the classified realm, and so I can't go any further into that.

BY MR. ABDO:

Q Let me just make sure I understand.

A Yep.

Q Is it true that the sentence we've been focusing on, the carryover sentence between pages 36 and 37 of Exhibit 43, is accurate as of 2014?

MR. PATTON: Objection, mischaracterizes prior testimony.

THE WITNESS: It is accurate, but incomplete, and that's a very important fact.

BY MR. ABDO:

Q And the reasons why it is incomplete you are saying are classified; is that correct?

A That is correct.

Q Is it incomplete because it omits additional information about the operation of upstream surveillance that is classified?

MR. PATTON: Let me just check to find

out whether the answer is yes or no.

(Counsel conferring.)

THE WITNESS: Ask your question one more -- can you repeat the question for me?

BY MR. ABDO:

Q I can ask it again.

Is the sentence that carries over between pages 36 and 37 of Exhibit 43 incomplete, which is the word you used --

A Correct.

Q -- because it omits information about the operation of upstream surveillance that is classified?

MR. PATTON: Just a second.

You can answer yes or no.

THE WITNESS: Okay, yes.

BY MR. ABDO:

Q Is it incomplete for any other reason other than that it omits additional information that is classified about the operation of upstream surveillance?

MR. PATTON: Object to form, but you

can answer.

THE WITNESS: It is incomplete because it omits classified information.

I'm not sure I understood your second question, what you were trying to -- what my other -- what other options you're providing for.

BY MR. ABDO:

Q A statement could be incomplete for a number of reasons. It could be incomplete because it omits relevant information, it could be incomplete because it includes information that is inaccurate or misleading, and I'm trying to understand why the NSA believes this sentence is incomplete?

A It's incomplete because it omits the classified information.

Q And for no other reason?

A Not that I can think of. I'm pausing because I can't -- I guess maybe you can be more specific, but I guess you said I could have added more information in -- they could have added more information into it and that's what makes it

incomplete? I'm not sure I understand. I guess I don't understand beyond omitting.

I'm willing say to say it's incomplete because it's omitting information. I'm not sure I understand the remainder of what you're trying to get at, so maybe you can rephrase it.

Q Let me ask it another way.

Is any of the information included in this sentence -- again, the sentence carrying over from pages 36 to 37 of Exhibit 43 -- inaccurate?

MR. PATTON: Objection, vague as to time.

MR. ABDO: As to the operation of upstream surveillance in 2014.

THE WITNESS: As I've said, it's incomplete.

BY MR. ABDO:

Q I'm asking if it's inaccurate.

A No. I've stated it's accurate. It's just incomplete.

Q Is it inaccurate as to the operation of upstream surveillance today?

MR. PATTON: Objection, calls for information that is classified and subject to the state secrets privilege, the other statutory privileges. I instruct the witness not to answer the question.

BY MR. ABDO:

Q Are you going to follow your lawyer's instruction not to answer?

A I'm going to follow my lawyer's direction not to answer.

Q Do you know the answer to the question that I asked? In other words, if you were to answer, could you?

A It would be classified, so I can't answer it because it's classified.

Q But do you know the information that you would provide in response but for --

A The classification?

Q Yes.

A Yes.

Q Is there anything you can say in response to the question without revealing

information you've been instructed not to provide?

A I would point you to the answer to the response that's on page 9 of the RFA, which accurately, to the extent possible given the classified nature, describes the current way Upstream works. And so I would -- that's how I would answer.

Q But specifically with respect to this sentence, is there anything you can say in response to my question, which was is the sentence accurate as to the operation of upstream surveillance today?

Is there anything you can say, aside from pointing me to other testimony or other information, that would not require you to disclose classified information?

A No.

Q Can you describe -- well, let me ask you this. Do you agree with your lawyer's instruction that answering the question would harm national security?

MR. PATTON: I'm going to object to

the form of the question as it seeks a legal conclusion, and as my colleagues just pointed out, beyond the scope of 30(b)(6).

MR. ABDO: You should take a look at guideline 7 of Appendix A of the local rules, which clearly contemplates counsel asking for the basis of assertions of privilege.

So my question is --

MR. PATTON: Same objection. That calls for a legal conclusion.

BY MR. ABDO:

Q Do you believe that answering the question would result in harm to national security?

A Yes.

Q Can you describe that harm?

MR. PATTON: No. I'm going to object to that question, as it would call for classified information and information subject to the statutory privileges, and I'll instruct her not to answer the question.

BY MR. ABDO:

Q Do you agree that describing the harm would itself result in harm to national security?

A Yes.

Q Have you discussed the invocation of the state secrets privilege with respect to this question with Admiral Michael Rogers?

MR. PATTON: With respect to this particular question?

MR. ABDO: Yes.

THE WITNESS: The question being -- I'm sorry, so just explain to me. The question is whether describing the difference between the sentence on page 36 and the interrogatory -- or the Request for Admission on page 9, whether describing what is different between those two would be a national security harm with him specifically?

BY MR. ABDO:

Q No. The original question was whether the carryover sentence from page 36 to 37 of Exhibit 43 is accurate with respect to upstream

surveillance as it is conducted today.

Have you discussed with Admiral Rogers whether answering a question seeking that information requires invocation of the state secrets privilege?

MR. PATTON: You can answer the question.

THE WITNESS: No, I have not.

BY MR. ABDO:

Q Have you more generally discussed the invocation of the state secrets privilege in this deposition with Admiral Rogers?

A I spoke to him extensively prior to the issuance of both the NSA Civil Liberties and Privacy Office Report, as well as the PCLOB Report, for him to understand what information was going to be in that.

So whether for today's testimony -- I did not go back to him and ask him specifically about any of this information, as that had largely been covered when we were issuing those reports back in 2014.

Q Okay. Is there anything else you can tell us about this assertion of the state secrets privilege?

MR. PATTON: Objection, vague.

THE WITNESS: I don't know what you're asking me.

BY MR. ABDO:

Q Is there anything that you can say that would be unclassified about the nature of the state secrets privilege invocation, or the reason for it, or the harm that would come about by answering the question?

A No, other than to say that this is sources and methods. You're getting into sources and methods, which is what we have -- we protect extensively.

Q Okay. As of 2014, did the NSA conduct upstream surveillance on at least one Internet backbone circuit?

MR. PATTON: Object to the question to the extent it calls for a classified answer, subject to the state secrets privilege, prior

statutory privileges.

You can answer the question to the extent not classified.

THE WITNESS: The question is at least one?

BY MR. ABDO:

Q Internet backbone circuit.

A One Internet backbone circuit.

MR. PATTON: This is probably another one of those questions where a yes-or-no answer would be unclassified, but --

MR. ABDO: That's what I'm looking for, a yes or no.

MR. PATTON: Any narrative answer we would have to break for.

THE WITNESS: At least one Internet --

BY MR. ABDO:

Q Let me restate the question.

A Okay.

Q As of 2014, did the NSA conduct upstream surveillance on at least one Internet backbone circuit? Yes or no.

MR. PATTON: Same classified objections to the extent that the question seeks classified information. To the extent it's yes or no, you can answer the question.

THE WITNESS: Yes.

BY MR. ABDO:

Q As of 2014, did the NSA conduct upstream surveillance on more than one Internet backbone circuit?

MR. PATTON: Object to that question to the extent it calls for classified information protected by the state secrets privilege, statutory privilege.

Instruct the witness not to answer the question.

THE WITNESS: I will follow my lawyer's direction.

BY MR. ABDO:

Q Your view is that stating a yes in response to that question or a no in response to that question would disclose state secrets?

MR. PATTON: Same objection, same

instruction.

THE WITNESS: Still following my lawyer's description -- direction.

BY MR. ABDO:

Q Is --

MR. GILLIGAN: Excuse me, Counsel, just one moment.

MR. ABDO: Yeah, sorry.

(Counsel conferring.)

BY MR. ABDO:

Q Is your view that the sentence we've been discussing between pages 36 and 37 of Exhibit 43 discloses any classified facts or facts protected by the statutory authorities your counsel has cited?

A The sentence is unclassified.

Q Is that true notwithstanding the fact that the sentence states that upstream surveillance involves the acquisition of communications transiting through circuits -- that's a quote -- on the Internet backbone?

MR. PATTON: Object to the form of the

question, vague as to time.

MR. ABDO: As of 2014.

MR. PATTON: Same objections, vague as to time.

THE WITNESS: My answer remains the same.

BY MR. ABDO:

Q What's your answer?

A That the fact that the word "circuits" is plural does not change any of my previous answers.

Q You don't view that as inconsistent with the assertion of the state secrets privilege in response to my question of whether, as of 2014, upstream surveillance involved more than one Internet backbone circuit?

MR. PATTON: Objection, asked and answered, argumentative. Go ahead.

THE WITNESS: I don't see that as inconsistent.

BY MR. ABDO:

Q Why not?

MR. PATTON: Same objections.

THE WITNESS: As we've stated, we've stated that we were on at least one, and the fact that there's a plural there isn't dispositive one way or the other.

BY MR. ABDO:

Q As of 2014, were multiple electronic communication service providers compelled to assist the NSA in the operation of upstream surveillance?

MR. PATTON: Objection, calls for classified information, sources and methods, operational details, and subject to state secrets and statutory privileges.

I instruct the witness not to answer the question.

THE WITNESS: I will follow my lawyer's --

BY MR. ABDO:

Q Can you please turn to page 12 of what's marked Exhibit 43 and read, if you would, what is marked as Recommendation 6, which is the

final paragraph of page 12.

MR. PATTON: Read it to herself or out loud?

MR. ABDO: To yourself, yeah.

THE WITNESS: Yes.

BY MR. ABDO:

Q Do you understand -- well, strike that.

Is it true that in the operation of upstream surveillance in 2014, there were -- and I'm quoting from this recommendation -- affected telecommunication service providers?

MR. PADGETT: Could you read back the question?

(The reporter read back the question.)

MR. PATTON: I'm going to object to vagueness in terms of time, and object to the question to the extent it calls for classified information, sources and methods information protected by the statutory privileges.

The witness can answer the question to the extent unclassified.

BY MR. ABDO:

Q Let me specify with respect to time that I'm talking about July 2nd, 2014, the date of this report.

MR. PATTON: Same objections.

THE WITNESS: I'd like to go in the SCIF before I answer this question.

MR. PATTON: Okay.

MR. ABDO: Take a break.

(Off the record at 12:16 p.m.)

(Resume at 12:19 p.m.)

MR. PATTON: Same objections.

THE WITNESS: So as I said earlier, providing any information as to the number of telecommunication service provider beyond one is classified. Because this is temporally at one point, we can neither confirm nor deny that information, whether it was more than one. To the extent there was more than -- to the extent there is a program, there must be one.

BY MR. ABDO:

Q Can you tell us whether there have

been more than one provider involved, even if not more than one at the same time?

MR. PATTON: Objection, calls for classified information pursuant to the state secrets privilege. Instruct the witness not to answer, and to the statutory privileges.

THE WITNESS: I will follow my lawyer's direction.

MR. ABDO: Rodney, are you okay shortening that objection to something?

MR. PATTON: I'm trying.

MR. ABDO: Okay.

Ms. Jaques, do you mind marking this as Exhibit 44?

(Deposition Exhibit 44 was marked for identification.)

BY MR. ABDO:

Q Ms. Richards, you have in front of you what's been marked as Exhibit 44. Do you recognize that document?

A Yes, I do.

Q Did you draft this document?

A I did.
Q What is the document?
A The document is the NSA Director of Civil Liberties and Privacy Office Report, NSA's Implementation of Foreign Intelligence Surveillance Act, Section 702, dated April 16th, 2014. It's exactly four years old.
Q Did the NSA review this document for accuracy and classification?
A Did the NSA?
Q Yes.
A Yes, it did.
Q Was that review thorough?
A Yes, it was.
MR. PATTON: Objection, vague.
THE WITNESS: Sorry, too fast.
BY MR. ABDO:
Q What was the purpose of issuing this report?
A The purpose of issuing the report was to put on the public record a description from NSA's perspective of what the privacy protections

were in place as it relates to Section 702.

Q Was it important to the NSA in issuing Exhibit 44 that the report be accurate?

A Absolutely.

Q And why is that?

A Because this was submitted to the Privacy and Civil Liberties Oversight Board as part of their request for comment as part of their report on Section 702, and we wanted to put on the record an unclassified description that NSA stood behind as to how the program worked.

Q And was it also important that the report, to the extent publicly disclosed, not reveal classified information?

A Yes.

Q Could you turn to page 5 of the report, again what's marked as Exhibit 44? I want to direct your attention to the first sentence of the last paragraph of the page, which starts, "In the second."

A Mm-hmm.

Q Could you read that sentence to

yourself, please, and let me know when you're done.

A (Witness reviewing document.) Okay.

Q Is this sentence referring to upstream surveillance as it operated as of April 16, 2014?

A Yes, it is.

Q Does this sentence confirm that service providers, plural, are compelled to assist the NSA in the lawful interception of electronic communications to, from, or about task selectors as of April 16th, 2014?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PADGETT: Can you read back the question?

(The reporter read back the question.)

BY MR. ABDO:

Q Let me ask it differently.

Is this sentence accurate as of April 16, 2014?

A To the extent, as with the PCLOB report, it's necessarily incomplete. It is

accurate to the outline of how the program works.

Q When you say it's incomplete, is it incomplete because it omits classified information about the operation of upstream surveillance as of April 16, 2014?

A Yes.

Q Is it incomplete for any other reason?

A No.

Q Do you understand this sentence to confirm that service providers are compelled to assist NSA in the lawful interception of electronic communications to, from, or about task selectors as of April 16th, 2014?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: We need to take just, I promise, a very short break to make sure the answer is unclassified. Thanks.

(Off the record at 12:26 p.m.)

(Resume at 12:40 p.m.)

MR. ABDO: Do you mind reading back the last question to us, Ms. Jaques?

(The reporter read back the question.)

MR. PATTON: Objection, vague as to time, and objection to the extent it seeks classified and otherwise statutorily privileged information.

You can answer to the extent it's unclassified.

THE WITNESS: So this sentence -- here's the thing. Would it have been clearer if we had put parens between the S? Yes. But we're not here -- we can't confirm or deny whether -- we've said that there was one service provider, at least one service provider in Upstream. The fact that this is plural does not -- is not an indication that it was more than one at that point in time or less than one at that point in time.

And so this is just -- it probably would have been clearer if we had put the parens. We didn't put the parens, so you've found the S's in our report, but it's not meant to have provided classified information, the fact that the numbers are classified.

BY MR. ABDO:

Q You understand that at the time that this report was issued -- and for the record, we're talking about Exhibit 44 -- there was a relatively small amount of unclassified information available from the government about the operation of upstream surveillance, right?

MR. PATTON: Objection, vague.

THE WITNESS: Yes, that's why I wrote the report.

BY MR. ABDO:

Q And you understand that the public and the PCLOB, which received this report, would regard it as an authoritative source of public information from the government about the operation of upstream surveillance?

MR. PATTON: Objection, calls for speculation about others and their thought processes.

THE WITNESS: Yes.

BY MR. ABDO:

Q And that was precisely one of the

reasons that you drafted it and disclosed the report, right?

A Correct.

MR. PATTON: Objection.

BY MR. ABDO:

Q Were you careful throughout to ensure that the factual assertions in this report were accurate?

MR. PATTON: Objection, vague.

THE WITNESS: Yes.

BY MR. ABDO:

Q And was that in part at least so as not to mislead the public or the PCLOB as to the operation of upstream surveillance at the time the report was issued?

A Yes.

Q Did you take great care throughout the rest of the report in every word used to ensure that what the words conveyed were accurate and unclassified?

MR. PATTON: Objection, vague.

THE WITNESS: Yes.

BY MR. ABDO:

Q Was this sentence reviewed with that same level of care?

MR. PATTON: Objection, vague.

THE WITNESS: Yes.

BY MR. ABDO:

Q Are you aware of any factually incorrect statements in Exhibit 44 as to the operation of upstream surveillance at the time that the report purports to describe the operation of upstream surveillance?

MR. PATTON: Objection, ambiguous.

MR. ABDO: I'm sorry, I didn't hear.

MR. PATTON: Objection, ambiguous.

THE WITNESS: Again, to the extent that the information in here is unclassified, and therefore is necessarily incomplete, yes, this is an accurate description.

This was also really one of the first times that the NSA had written, so to the extent we've gotten better at this as we've gone along, the first time is always -- we were doing our

best.

BY MR. ABDO:

Q Setting aside the question of incomplete information, are you aware of any factual inaccuracies in Exhibit 44 as to the operation of upstream surveillance at the relevant time periods described in the report?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: Go ahead.

THE WITNESS: No, I'm not.

BY MR. ABDO:

Q Also setting aside the question of incompleteness, are you aware of any factual inaccuracies in Exhibit 43, the report of the PCLOB, as to the operation of upstream surveillance for the periods of time described in that report?

MR. PATTON: Objection, vague.

THE WITNESS: As I said earlier, and as we just then described going through these different sentences, the answer is I am not

generally aware of any inaccuracies.

To the extent you have a question about a particular sentence, I'm happy to, as we did on page 36, walk you through and understand whether there was classified information that makes that sentence more or less complete.

BY MR. ABDO:

Q I appreciate that, and we may do that for a few more sentences, but my question is whether, as you sit here today, you are aware of any inaccuracies, factual inaccuracies, in Exhibit 43 with regard to the operation of upstream surveillance as the report describes?

MR. PATTON: Objection, asked and answered.

THE WITNESS: My answer is still the same. You know, the information in it is, generally speaking, accurate.

If there's a particular sentence you want to discuss -- it's necessarily incomplete, and describing Upstream, which is classified, in an unclassified sentence is difficult, as you're

seeing with us having to walk back and forth and make sure that we're hitting those lines so that we are providing an accurate general description of the program without going into the classified sources and methods of the program.

So, you know, it still remains accurate to the extent that it was true in 2014. I'll just re-remind you that we are no longer do the "abouts" collection as it was described starting in 2017, and so that piece of this report is not accurate.

BY MR. ABDO:

Q The report doesn't purport to describe surveillances operated years later, correct?

A Correct. I'm just re-reminding that to the extent that we've changed certain aspects of the program, that's no longer accurate.

Q Okay. I'm going to ask you similar questions that I just asked you about Exhibit 44, but about Exhibit 43.

Did the NSA, as it did with Exhibit 44, also review each and every factual

disclosure in Exhibit 43 to ensure that it was accurate?

MR. PATTON: Object to the form, vague, asked and answered.

THE WITNESS: To the extent that NSA scrubbed through the facts provided in the historical, as we mentioned, section from 16 to roughly 79, and also looked at from a classification purpose, yes.

We were, again, doing our best to try and help provide an unclassified description of a classified program, and so it was necessarily incomplete.

BY MR. ABDO:

Q And at the time that report was issued, is it also fair to say that there was relatively little public information from the government describing the operation of upstream surveillance?

MR. PATTON: Object to the form, vague.

THE WITNESS: I'm pausing because I

don't exactly remember when a number of the different FISC opinions were declassified. So I believe that there were a number of -- they were actually issued -- that they were declassified prior to -- or they were reviewed and redacted.

So Judge Bates -- which are mentioned. There are a number of reports that are footnoted in here that are -- that were declassified. I just -- some of the timing.

BY MR. ABDO:

Q Is it fair to say that at the time this report was issued, it was the most comprehensive description from the government of how upstream surveillance operated at the time the report was issued?

MR. PATTON: Objection, vague.

THE WITNESS: Yes, to the extent, though -- I would just offer that to the extent that these are the words of an independent executive agency with oversight over the Intelligence Community as it relates to CT functions, you know, these are their words.

They're not NSA's words. They're not NSA submissions.

And so sometimes they may describe things slightly differently than we may have chosen to do so, and so I would refer you back to the NSA or the government submissions on the descriptions of the programs.

BY MR. ABDO:

Q Okay. Is it fair to describe the report marked Exhibit 43 as an exhaustive description of upstream surveillance as it operated in 2014?

MR. PATTON: Objection, vague.

THE WITNESS: I suppose that's one. I'm guessing that you have something over there that -- are you referring to a specific document where NSA may have said that?

BY MR. ABDO:

Q Well, I'm asking you first whether that's fair, setting aside what the NSA has otherwise said?

A Yes, I think it's fair.

MR. PATTON: In unclassified terms.

THE WITNESS: In unclassified terms.

MR. PATTON: I guess that's probably what that's talking about, right?

MR. ABDO: Yeah, no, I think -- let me ask the question clearly.

Is the PCLOB's description of the operation of upstream surveillance exhaustive?

MR. PATTON: Same objection.

THE WITNESS: So, again, I think what I would say is I think that their study was exhaustive. To the extent that there's classified information, they had access to that information, which makes the study probably exhaustive, but to the extent that the report is necessarily incomplete, it's as much information as possible without going into the classified material.

BY MR. ABDO:

Q Okay. I want to ask you a question that I've tried different versions of, so forgive the repetition. I'm asking it multiple ways because I'm looking for what I think you ought to

be able to provide, which is a clean yes or no.

Setting aside the incompleteness of the report marked Exhibit 43, are you aware now of any factual inaccuracies in the report and its description of upstream surveillance as Upstream was conducted at the time the report was issued?

MR. PATTON: Objection, asked and answered. Go ahead.

THE WITNESS: I am not aware of any inaccurate -- known inaccuracies in the document as described other than the fact that there's classified information that has been omitted.

BY MR. ABDO:

Q What is the number, or approximate number, of Internet backbone circuits on which upstream surveillance is conducted --

MR. PATTON: Objection.

MR. ABDO: -- as of June 2015?

MR. PATTON: Objection, calls for classified information, sources and methods, operational details subject to state secrets and the statutory privilege.

Instruct the witness not to answer.

THE WITNESS: I will follow my lawyer's direction.

MR. ABDO: Rodney, I think it might be in our interest to come up with a shortened version of that, at least for the next few minutes.

MR. PATTON: Yes, you have my word.

BY MR. ABDO:

Q What is the number, or approximate number, of Internet backbone circuits on which upstream surveillance is conducted today?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Still following those directions.

BY MR. ABDO:

Q Okay. What is the average bandwidth of the Internet backbone circuits on which upstream surveillance was conducted in June 2015?

MR. PATTON: Same objections, same instruction.

THE WITNESS: Following the instruction.

BY MR. ABDO:

Q What is the average bandwidth of the Internet backbone circuits on which upstream surveillance is conducted today?

MR. PATTON: Same objections, same instruction.

THE WITNESS: Still following the instructions.

BY MR. ABDO:

Q What is the approximate combined bandwidth of the Internet backbone circuits on which upstream surveillance was conducted in June of 2015?

MR. PATTON: Same objections, same instruction.

THE WITNESS: Still following instructions.

BY MR. ABDO:

Q What is the approximate combined bandwidth of the Internet backbone circuits on

which upstream surveillance is conducted today?

MR. PATTON: Same objections, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q What are the categories of circuits that were subject to upstream surveillance in June 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q What are the categories of circuits that are subject to upstream surveillance today?

MR. PATTON: Same objections, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q Were any individual optical fibers on the Internet backbone subjected to upstream surveillance in June 2015 and/or any individual optical fibers on the Internet backbone subjected

to upstream surveillance today?

MR. PATTON: Just a second.

MR. PADGETT: Could you read back the question?

MR. ABDO: Sure. Let me --

MR. PATTON: I really am listening to your questions.

BY MR. ABDO:

Q I appreciate that. In the interest of speed, I was combining two, but let me be clear.

Are any individual optical fibers on the Internet backbone subjected to upstream surveillance today?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q Were any individual optical fibers on the Internet backbone subjected to upstream surveillance as of June 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q Are any subdivisions of optical fibers on the Internet backbone subjected to upstream surveillance today?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q Were any subdivisions of optical fibers on the Internet backbone subjected to upstream surveillance in June 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q Are any wavelengths of light carried on optical fibers on the Internet backbone subjected to upstream surveillance today?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q Were any wavelengths of light carried on optical fibers on the Internet backbone subjected to upstream surveillance in June 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q What is the smallest subdivision by bandwidth of an optical fiber on the Internet backbone that was subjected to upstream surveillance in June 2015 and that is subjected to upstream surveillance today?

MR. PATTON: Objection, compound. Objection, same as before, classified.

MR. ABDO: We might go quicker if you would withdraw the compound objection.

MR. GILLIGAN: I like this pace, actually.

BY MR. ABDO:

Q Let me rephrase the question.

What is the smallest subdivision by

bandwidth of an optical fiber on the Internet backbone subjected to upstream surveillance today?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q What was the smallest subdivision by bandwidth of an optical fiber on the Internet backbone subjected to upstream surveillance in June 2015?

MR. PATTON: Same instruction, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q What was the largest circuit by bandwidth on the Internet backbone subjected to upstream surveillance in June 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q What is the largest circuit by

bandwidth on the Internet backbone subjected to upstream surveillance today?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q Is now a good time for you to break, Ms. Richards?

A Sure.

Q Okay, why don't we take a lunch break and go off the record, Dawn.

(Lunch break taken at 12:59 p.m.)

(Resume at 2:06 p.m.)

BY MR. ABDO:

Q We're back from lunch.

Ms. Richards, what does the term "Internet link" refer to?

MR. PATTON: Objection, vague.

THE WITNESS: Is there a specific place where you want me to look for "Internet link," or are you looking for the general telecommunications definition?

BY MR. ABDO:

Q That's right, the general definition.

A So it's similar to a circuit, and there's no special NSA meaning.

Q So the NSA's understanding of that term is consistent with the general understanding of the term within the telecommunications industry?

A That is correct.

Q Okay. What does the term "international Internet link" refer to?

MR. PATTON: Objection, vague, calls for expert opinion.

THE WITNESS: I'm sorry, international --

BY MR. ABDO:

Q International Internet link.

A Is there, again, something specific? I'm not sure of it.

Q The question is whether that term has a meaning to the NSA.

MR. PATTON: Just a second.

I'm just going to object to the extent that any response might call for a classified answer, subject to state secrets, statutory privileges.

If the witness has an unclassified answer, she can provide it.

THE WITNESS: I'm just going to take a minute to make sure I --

(Witness reviewing document.)

So just for clarification, you're looking for the definition of "international Internet link" --

BY MR. ABDO:

Q That's right.

A -- as was originally described in Judge Bates' order?

Q I'm asking for your understanding of it, not for Judge Bates' understanding.

A Okay, I just want to make sure.

So I'll say there's no special NSA meaning.

Q What is the meaning of it though, even

if there's not a special NSA one?

MR. PATTON: Objection to the extent it calls for expert opinion, and to the extent it may call for classified information and statutory privileges.

The witness can answer if the answer is unclassified.

Are you concerned that there's --

THE WITNESS: I'm concerned whether I'm going into classified. I'm just trying to under- -- I'm clicking through my head as to what's classified and what's not classified, so I'm sorry I'm taking a little bit more, and so maybe --

MR. PATTON: Do you need to talk about that?

THE WITNESS: Maybe we should just take a quick minute, go off the record.

MR. ABDO: Okay.

(Off the record at 2:11 p.m.)

(Resume at 2:28 p.m.)

MR. ABDO: Ms. Jaques, do you mind

re-reading the last question asked?

(The reporter read back the question.)

MR. PATTON: Object to the question to the extent it calls for expert testimony.

THE WITNESS: I'm going to clarify my answer, which is the logical definition of an international Internet link would be an Internet link between two countries, but it's not I think a well -- it's not a telecommunications -- unlike some of the other descriptions that we provided in terms of "circuit" or "cable" or "Internet backbone," this is not a commonly understood telecommunications word -- or set of three words, I guess.

BY MR. ABDO:

Q Okay. But your understanding of it is a link between two countries essentially?

MR. PATTON: Same objection.

THE WITNESS: Yes, in the broad context of those three words, not in the context of anything specific.

BY MR. ABDO:

Q Okay. I want to go back for a moment to Internet link -- not international Internet link, just Internet link.

You said, I believe, and please correct me if I'm wrong, that it is similar to a circuit. Is that correct? Am I characterizing your previous testimony accurately?

MR. PATTON: Object to the extent it calls for expert opinion.

THE WITNESS: Yes.

BY MR. ABDO:

Q When you say "similar" -- or when you said "similar," did you mean analogous to, or did you mean identical to? I'm trying to understand, if there are differences between an Internet link and a circuit, what you believe those differences to be.

MR. PATTON: Same objection.

THE WITNESS: I don't see them -- I see them as being analogous. So sometimes you use "circuit," sometimes you use "link." I don't see

them as having any real difference between them.

BY MR. ABDO:

Q Okay. Would "interchangeable" be a better word than "analogous" then?

A Yeah.

MR. ABDO: Ms. Jaques, would you mind marking this Exhibit 45?

(Deposition Exhibit 45 was marked for identification.)

BY MR. ABDO:

Q Ms. Richards, you have in front of you what's been marked as Exhibit 45.

Do you recognize that document?

A I do.

Q What is it? I should say, sorry, it's marked Exhibit 45, and it is Bates numbered NSA-WIKI 149 to NSA-WIKI 229. Wiki is spelled W-I-K-I. What is this document, Ms. Richards?

A This is the Judge Bates' Memorandum Opinion from October 3rd, 2011.

Q Could you turn to page 45, or NSA-WIKI 193 of Exhibit 45, and read the sentence

that begins, "Indeed, the government readily concedes." It is about halfway down the page.

A Got it.

Q "Indeed, the government readily concedes that NSA will acquire a wholly domestic 'about' communication if the transaction containing the communication is routed through an international Internet link being monitored by NSA or is routed through a foreign server."

Is that sentence true?

Let me rephrase that. Was that sentence true at the time Judge Bates issued this opinion?

MR. PATTON: Just a moment.

You can answer.

THE WITNESS: Okay. Yes, that sentence is accurate.

BY MR. ABDO:

Q What do you understand the Foreign Intelligence Surveillance Court to mean in its use of the term "international Internet link" in that sentence?

MR. PATTON: Objection, the question calls for classified information, information subject to the state secrets and the statutory privileges previously mentioned.

I instruct the witness not to answer the question.

BY MR. ABDO:

Q Do you --

A Hold on.

MR. PATTON: Do you have an unclassified response?

THE WITNESS: I have an unclassified response, at least in part.

MR. PATTON: So long as you're comfortable and it's unclassified.

THE WITNESS: NSA -- so unlike the other words that you had me go through in terms of definitions that were telecom provider -- you know, sort of generally what a teleco expert would be, NSA has an understanding of this term that is specific to how Judge Bates described it, but it's classified to provide any further information.

BY MR. ABDO:

Q I understand. Is the NSA's understanding of the term different from the general meaning of the term you described in response to an earlier question as a link between two countries?

MR. PATTON: Objection, calls for information subject to the statutory privilege, and instruct the witness not to answer the question.

THE WITNESS: I will follow instructions.

BY MR. ABDO:

Q Is it your understanding that in using the term "international Internet link," the Foreign Intelligence Surveillance Court meant an Internet link that terminates in a foreign country?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q Is it your understanding that an international Internet link is an Internet backbone circuit with one end in the United States and the other end in a foreign country?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q Is there anything you can tell us unclassified about the nature of the harm that would arise were you to provide an answer to the question of what the term "international Internet link" means as used by the Foreign Intelligence Surveillance Court in Exhibit 45?

MR. PATTON: Object to the question. The witness is not an official classification authority, nor is she the Director of the NSA or the Director of National Intelligence, who would invoke and assert the state secrets privilege to that.

You can answer the question to the

extent it's unclassified.

THE WITNESS: Sources and methods.

BY MR. ABDO:

Q Do you believe that disclosing the NSA's understanding of that term would harm national security?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Which was to not answer, or to answer to the extent --

MR. PATTON: To answer to the extent that you're able. You're not a classification authority, you're not asserting the state secrets.

THE WITNESS: So the question is whether I believe it would harm national security?

BY MR. ABDO:

Q Yes.

A Yes.

Q Do you believe it would substantially harm national security?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Yes.

BY MR. ABDO:

Q Are you familiar with the process through which the government seeks approval from the Foreign Intelligence Surveillance Court to conduct upstream surveillance?

MR. PATTON: Object to the form of that question as vague, and objection, beyond the scope of 30(b)(6).

THE WITNESS: Yes.

BY MR. ABDO:

Q Does the NSA provide information to the Foreign Intelligence Surveillance Court about the operation of upstream surveillance in support of the government's applications to that court to conduct upstream surveillance?

MR. PATTON: Same objections.

THE WITNESS: Yes.

BY MR. ABDO:

Q Is the information that the NSA provides in support of the government's applications to the Foreign Intelligence

Surveillance Court supposed to be accurate?

MR. PATTON: Objection. Same objections.

THE WITNESS: Yes.

BY MR. ABDO:

Q Is that information, in fact, accurate?

MR. PATTON: Objection, calls for speculation.

THE WITNESS: To the extent the government's job is to provide the Court with as accurate as information as possible at the time, that is what the NSA does.

BY MR. ABDO:

Q Does the NSA verify, under penalty of perjury, that its submissions to the Foreign Intelligence Surveillance Court are true and correct?

MR. PATTON: Same objections.

THE WITNESS: Yes.

BY MR. ABDO:

Q Does the NSA review the Department of

Justice's submissions to the Foreign Intelligence Surveillance Court seeking authority to conduct upstream surveillance?

MR. PATTON: Same objections.

THE WITNESS: Yes.

BY MR. ABDO:

Q Does it review the technical explanations of the way that upstream surveillance operates and drafts of those submissions before they are filed with the Foreign Intelligence Surveillance Court?

MR. PATTON: Same objections.

MR. PADGETT: Excuse me, could you read back the question?

(The reporter read back the record.)

THE WITNESS: Okay, yes.

BY MR. ABDO:

Q If there are mistakes in the drafts of the Department of Justice's submissions to the Foreign Intelligence Surveillance Court, would the NSA identify those mistakes to the Department of Justice?

MR. PATTON: Objection, vague.

THE WITNESS: Yes.

BY MR. ABDO:

Q Would it identify any inaccuracies in the explanations of the technical operation or implementation of upstream surveillance to the Department of Justice?

A Yes.

MR. PATTON: Objection, vague and ambiguous, and also beyond the scope of 30(b)(6).

THE WITNESS: Yes.

BY MR. ABDO:

Q To your knowledge, does the Foreign Intelligence Surveillance Court acquire information about the operation of upstream surveillance from anyone aside from representatives of the NSA or the Department of Justice?

MR. PATTON: Objection, calls for speculation. Objection, beyond the scope of 30(b)(6).

THE WITNESS: What time frame would

you be asking about? Just in general? Over a specific time frame?

BY MR. ABDO:

Q Why don't we -- if you can answer in general, please do. If you can't, let me know.

MR. PATTON: Are you asking -- I'm sorry, does this include just Upstream?

MR. ABDO: Just Upstream.

MR. PATTON: Same objections.

THE WITNESS: To the extent that the new law that was passed, and actually some previous ones over the last couple years, allow for an Amicus, there's certainly that opportunity for the Court to include that type of additional expert outside advice. Similarly -- yeah.

BY MR. ABDO:

Q The new law you're referring to is the USA Freedom Act?

A Yes. I'm sorry, yes, USA Freedom Act, and then the --

Q The reauthorization --

A -- reauthorization for 702 also has

the Amicus portion of it.

Q Is there anyone else, to your knowledge, from whom the Foreign Intelligence Surveillance Court might acquire information about the operation of upstream surveillance?

MR. PATTON: Same. Hold on.

(Counsel conferring.)

MR. PATTON: So same objections as before. There are, as you know, some ex parte communications, and while I'm a Department of Justice Civil Division attorney, I'm not a Department of Justice national Security Division attorney, and so there may be other things that the witness is not aware of.

Again, I'd objected before to the fact that the it was beyond the scope of 30(b)(6), so she may not be aware of certain other things that may go on that I'm not aware of as well. I don't want the record to be unclear. That's potentially beyond her personal knowledge.

MR. ABDO: Understood. To the extent you know the answer --

THE WITNESS: So his answer was exactly what I was about to say before we -- before my lawyer said that, which is fantastic, so I've given you the information I know.

I don't work for the FISC, I don't do anything before the FISC, so what the FISC -- what else the FISC has at their disposal is up to the FISC.

BY MR. ABDO:

Q Do you know whether the NSA reviews or participates in any review of opinions of the Foreign Intelligence Surveillance Court concerning upstream surveillance before those opinions are signed or issued?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: Would you just read that back? I think it's fine, but I just want to be double sure.

(The reporter read back the question.)

MR. PATTON: Object as beyond the scope of 30(b)(6), but if you have personal

knowledge, you can give it.

THE WITNESS: To the best of my knowledge, no.

BY MR. ABDO:

Q If the NSA identifies an inaccuracy in an opinion of the Foreign Intelligence Surveillance Court concerning upstream surveillance after that opinion is issued, would the NSA notify the Foreign Intelligence Surveillance Court of that inaccuracy?

MR. PATTON: Objection. Same as before, beyond the scope of 30(b)(6).

You can answer if you know.

THE WITNESS: I think that's when you would go to the FISC Review Board. You would do an appeal.

BY MR. ABDO:

Q What if it were not a judgment that the Department of Justice or the NSA disagreed with, but a factual misstatement in the opinion that would not give rise to or necessitate an appeal?

MR. PATTON: Same objection.

THE WITNESS: It would be fact specific. I can't speak to one way or another.

BY MR. ABDO:

Q Okay. Do you imagine that it would be good practice for the NSA to correct factual misstatements in the Foreign Intelligence Surveillance Court's opinions if and when they identify them?

MR. PATTON: Objection, calls for a legal conclusion, opinion, speculation, and beyond the scope of 30(b)(6).

THE WITNESS: Again, I think it would have to be very fact specific -- you know, the sort of situation and fact specific would have to decide what to do next, but, I mean, it's an Article III judge signing something. We're not really one part of the government saying something to the other part of the government. You may want to be thoughtful about how to do that.

BY MR. ABDO:

Q Understood. Are there any

inaccuracies that you're aware of relating to the operation of upstream surveillance in Exhibit 45, October 3rd, 2011, Foreign Intelligence Surveillance Court opinion?

MR. PATTON: Objection, vague as to time, and object to the extent it calls for classified information or statutory privileges information.

The witness can answer to the extent unclassified.

THE WITNESS: So you're asking if there's any information as of October 3rd, 2011, that we believe would have been inaccurate in Judge Bates' Memorandum and Opinion?

BY MR. ABDO:

Q Yes.

A To the extent that there are certain opinions that the judge makes as it relates to different aspects of this, those are the opinions of the Court and not necessarily those of NSA.

To the extent that there are facts in here, I believe we stand behind those facts, as

they're based off of the submission from June 1st that the government made in the subsequent submissions.

Q Okay. Did the NSA conduct a declassification review of Exhibit 45?

A Yes.

Q I assume that was a thorough review?

A Yes.

Q And anything that would disclose classified information, the NSA would identify as classified to the FISC so as not to release it to the public?

MR. PATTON: Just a second.

(Counsel conferring.)

MR. PATTON: I'm sorry, could you read that question back?

BY MR. ABDO:

Q Let me rephrase it. That's all right.

Did the NSA -- sorry.

If the NSA identified classified information -- let me -- sorry, let me start over.

Who actually disclosed Exhibit 45 to

the public?

MR. PATTON: Objection, vague.

THE WITNESS: It's a FISC document, so while the government has -- while the Executive Branch reviews it for classification, I believe the FISC issues it, although I know that the documents actually sit on ODNI's website.

BY MR. ABDO:

Q Are the redactions in this opinion in Exhibit 45 the government's redactions or the FISC's redactions?

A So the process is with all these documents that the government -- the Executive Branch will review them for classification and suggest redactions, and then the FISC has the opportunity to say no, I think these should be put out, and there was a conversation. But as a general matter, I guess they're really the FISC's document.

Q Do you know whether there's any dispute between the NSA or the Department of Justice with the FISC relating to the

classifications in Exhibit 45?

MR. PATTON: Just a second.

(Counsel conferring.)

MR. PATTON: My colleague was just getting warm. You can keep answering the question.

THE WITNESS: Okay.

MR. PATTON: I think there's some confusion back and forth as to this particular document, when it was declassified, and then the standard way that it's now under USA Freedom Act taken care of.

But this was, as you know, declassified prior to USA Freedom Act, and so I want to make sure the witness's answers are both accurate and reflective of what occurred.

BY MR. ABDO:

Q Right. I'm asking specifically about this opinion, Exhibit 45.

A And to which I don't know. I was not working at NSA. This I believe was declassified in 2013, and I was not working at NSA at that

point, so I don't have any specific knowledge on that fact.

Q Is there somebody at NSA who would know the answer to that question?

A I imagine the answer is that there wasn't any disagreement, that this is the document that went out.

Q Just to confirm though, you say you imagine that. Is that a guess, or is that --

A No, that's a statement. I mean, this is the document that went out. If there were any disagreements, those were resolved.

Q Okay.

A There's no further information that can be provided as to what those would be or not be.

Q Okay. Would the NSA treat statements in a FISC opinion as classifiable if they revealed information that the government considered classified?

MR. PATTON: Objection to the question. It calls for the expertise of an

original classification authority, and it's beyond the scope of 30(b)(6). You can answer.

THE WITNESS: I'm not sure I understand your question, so ...

BY MR. ABDO:

Q Let me ask it a slightly different way.

Would the NSA treat a statement in a FISC opinion as classifiable if it revealed information the government considered classified even if the FISC were not quoting a statement made by an Executive Branch agent?

MR. PATTON: Objection.

BY MR. ABDO:

Q In other words, if the FISC were to make a factual statement using its own words about the operation of upstream surveillance, and the NSA believed that statement revealed classified information, would the NSA consider that statement to be classifiable?

MR. PATTON: Same objections.

THE WITNESS: Yes.

BY MR. ABDO:

Q Okay. Does the NSA conduct upstream surveillance on one or more international Internet links? I'm looking for a yes or no, not a specific number.

(Counsel conferring.)

MR. PADGETT: Could you read it back?

(The reporter read back the question.)

MR. PATTON: I misheard, so object to that as seeking classified information, subject to state secrets and statutory privileges.

Instruct the witness not to answer the question.

THE WITNESS: I'll follow the --

BY MR. ABDO:

Q Did the NSA conduct upstream surveillance on one or more international Internet links in 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow instruction.

BY MR. ABDO:

Q Does the NSA conduct upstream surveillance today on more than one international Internet links?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. ABDO:

Q Did the NSA conduct upstream surveillance on more than one international Internet links in June of 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Follow the instruction.

BY MR. ABDO:

Q What is the number or approximate number of international Internet links on which the NSA conducted upstream surveillance in June of 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the direction.

BY MR. ABDO:

Q What is the approximate number of international Internet links on which the NSA today conducts upstream surveillance?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow instruction.

BY MR. ABDO:

Q Okay. Is upstream surveillance conducted on any international submarine cables?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow instructions.

BY MR. ABDO:

Q Was upstream surveillance conducted on any international submarine cables in June of 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow instruction.

BY MR. ABDO:

Q What is the number or approximate number of cables on which the NSA conducted upstream surveillance in June 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow instruction.

BY MR. ABDO:

Q What is the number or approximate number of cables on which the NSA today conducts upstream surveillance?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow instruction.

BY MR. ABDO:

Q Okay. In the context of upstream surveillance, can you tell me what an international chokepoint is?

MR. PATTON: Just a second.

Will you just read it back, please?

(The reporter read back the question.)

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. ABDO:

Q Is upstream surveillance today conducted at one or more international chokepoints?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow instruction.

BY MR. ABDO:

Q Was upstream surveillance in June 2015 conducted at one or more international chokepoints?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. ABDO:

Q What number, approximate number, of international chokepoints was upstream

surveillance conducted on in June 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow instruction.

BY MR. ABDO:

Q What number, approximate number, of international chokepoints is upstream surveillance conducted on today?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow instruction.

BY MR. ABDO:

Q I want to go back to page 45 very briefly of Exhibit 45, the sentence we were talking about before, the one that begins, "Indeed, the government readily concedes."

A Yes, okay.

Q Is there a term -- well, let me scratch that for a moment.

A moment ago I asked you whether the government conducts upstream surveillance on one or more international Internet links in 2015, then

I asked about today.

Is there a way I could phrase that question that would allow you to respond with an unclassified response more fully than you've responded so far?

MR. PATTON: For any given time period?

MR. ABDO: For June 2015 to today, and in 2011, at the time of -- let me try rephrasing one thing.

As of October 3rd, 2011, did the NSA conduct upstream surveillance on one or more international Internet links?

MR. PATTON: Same objection, same instruction.

BY MR. ABDO:

Q Is there a way that I could rephrase that question to use a term other than "international Internet link" that would allow you to provide an unclassified response?

(Counsel conferring.)

MR. PATTON: We don't think she can.

This is Rodney Patton, counsel for government.

We don't think she can answer that as to specific time periods for anything related to international Internet link. There may be a more general statement that she can make, but I feel like she's probably already provided that to you.

MR. ABDO: Okay.

MR. PATTON: Perhaps if we could go out and check, we might be able to come up with --

MR. ABDO: Maybe at the next break. You can add this to --

MR. PATTON: That's fine.

BY MR. ABDO:

Q So back to page 45 very briefly of Exhibit 45. Do you understand the sentence we've been discussing, the one that begins, "Indeed, the government readily concedes," to confirm that, as of October 3rd, 2011, that the government in fact conducted upstream surveillance at at least one international Internet link?

MR. PATTON: Objection, mischaracterizes the language of page 45 of

Exhibit 45.

BY MR. ABDO:

Q You can answer.

A Do you want me to answer?

MR. PATTON: Not as it's phrased, no, she can not answer that question. It would call for a classified answer.

MR. ABDO: I'm sorry, I didn't hear that. So you're instructing the witness not to answer?

THE WITNESS: Yeah, that's classified.

BY MR. ABDO:

Q Okay. Do you understand the sentence to confirm that if a transaction -- that as of October 3rd, 2011, the NSA would in fact acquire a wholly domestic -- sorry, would in fact acquire a wholly domestic "about" communication if the transaction containing the communication were routed through an international Internet link being monitored by the NSA?

MR. PATTON: Objection as not exactly what the language of the sentence said. Let me

see if she can answer that question.

To avoid us having to go out to the SCIF and come back again, she can answer whether or not the statement in this, as exactly written, is correct as of October 3rd, 2011, in a yes-or-no answer. I believe she's already answered that, but --

MR. ABDO: I think you did already answer that this sentence, as written, is true as of October 3rd, 2011.

MR. PATTON: That she can answer.

MR. ABDO: Okay.

THE WITNESS: Do you want me to say it again?

BY MR. ABDO:

Q Sure.

A Yes, that sentence is accurate as of October 3rd, 2011.

Q Okay. Let me go back to Exhibit 42.

A Which one is 42?

Q The NSA's Responses and Objections to Plaintiffs' First Set of Interrogatories.

I direct your attention to page 7 to 8.

A 7 to 8, oh, yes.

Q The paragraph that carries over between the two, which is labeled "RESPONSE."

Would you mind just reading that to yourself?

MR. ABDO: Why don't we take a break right now. Can we go off the record for a minute?

(A break was taken at 3:06 p.m.)

(Resume at 3:15 p.m.)

BY MR. ABDO:

Q Ms. Richards, have you had a chance to look at page 6 of Exhibit -- sorry, page 7 to 8 of the carryover paragraph on pages 7 to 8 of Exhibit 42, the NSA's response to Interrogatory No. 3?

A Yes.

Q Is there anything beyond that response in Exhibit 42 that isn't classified that you could provide us about the NSA's understanding of the term "filtering mechanism," both in June 2015 and

today?

A Those are pretty good definitions you've got right there. I don't have anything else to add.

Q Does that mean that there isn't anything unclassified that you could add to those definitions?

A There's nothing unclassified I can add to those descriptions.

Q Okay. With respect to upstream surveillance as it operated in 2015, did the term "filtering mechanism" include the use of, quote, an Internet protocol filter to ensure that the person from whom the NSA seeks to obtain foreign intelligence information is located overseas?

A In 2015, filtering mechanism would have -- one of the examples that was used -- I'm sorry.

An example of a filtering mechanism was an IP address -- sorry. (Reviewing document.)

Okay, let me revise -- I'm sorry, let me just revise my answer.

Q Sure.

A So I would actually add from the Civil Liberties and Privacy Office Report, which is Exhibit 44, on page 5, where we give an example that, in certain circumstances, NSA's procedures require that it employ an Internet protocol filter to ensure that the target is located overseas.

Q Does that mean the answer to my question is yes, that the filter you just described is part of the filtering mechanism described in the NSA's response to Interrogatory No. 3?

A Yes, and so I was correcting the fact that when I said that was everything you could say in an unclassified.

What I'm saying is I'm correcting the record to say I could have additionally added the fact that that would include the IP -- that could include -- could include --

Q Could include, understood.

A -- as an example of what the filtering mechanisms are, so ...

Q In June of 2015, did the term "filtering mechanism" include the use of an Internet protocol filter? I'm trying to understand "did" versus "could" include.

MR. PATTON: Just a second.

(Counsel conferring.)

MR. PATTON: Object to form, vague.

You can answer.

THE WITNESS: Okay. To the extent that the information is classified -- to the extent that how this exactly works is classified, I use the term "could" as one of the examples of what a filtering mechanism is.

I can neither confirm nor deny exactly what was happening in 2015 as it relates to the specificity of the filtering mechanism. I can just tell you that it could include that as an example.

BY MR. ABDO:

Q Can you confirm whether it did include an Internet protocol filter as of the date of Exhibit 44, April 16th, 2014?

A As is specifically stated on page 5, it's a "could." It's not a "did."

Q Just for the record, could you tell us where you're reading from on page 5?

A Sure. It's the very last sentence on page 5 of Exhibit 44 that begins with "for example."

Q "In certain circumstances, NSA's procedures require that it employ an Internet protocol filter to ensure that the target is located overseas."

So in certain circumstances, they're required to.

A Mm-hmm.

Q Can you tell us what those certain circumstances would be in unclassified terms?

MR. PATTON: No, she can't. Object to the question to the extent it calls for classified information --

THE WITNESS: The information -- oh.

MR. PATTON: -- subject to the state secrets and statutory privileges, and instruct the

witness not to answer.

THE WITNESS: I'll follow.

BY MR. ABDO:

Q With respect to upstream surveillance as it operated in 2015, did the term "filtering mechanism" include, quote, the use of a screening device in the upstream Internet collection process to acquire only Internet transactions containing at least one task selector?

A It appears you're reading from something. Could you just refer me to where those words exactly are to make sure I have the full context?

Q Sure. The last portion of my question was a direct quote from the NSA's response to Interrogatory No. 5 in Exhibit 42 on page 10, the text marked "RESPONSE."

A Okay. And so could you read your question once more?

Q With respect to upstream surveillance as it operated in 2015, did the term "filtering mechanism" include, quote, the use of a screening

device in the upstream Internet collection process to acquire only Internet transactions containing at least one task selector?

A So I would look at Interrogatory 4. I understand you pointed me to the response to Interrogatory 5, but the process is we filter for wholly domestic communications, and then we do the scanning to ensure that we're only -- we're doing a scan using a screening device designed to identify for acquisition Internet transactions.

And in 2015, it would have been to, from, or about persons targeted; today, it's to or from persons targeted, in parens, with our targeting procedures.

Q Okay. What I'm trying to understand is whether the use of a screening device is part of the filtering mechanism process described in NSA's response to Interrogatory 3?

MR. PATTON: Objection, calls for information that's classified, subject to state secrets and statutory privileges.

Instruct the witness not to answer.

THE WITNESS: Follow instruction.

BY MR. ABDO:

Q Would you be able to answer the question if I asked whether the use of a screening device could be part of the filtering mechanism described in the NSA's response to Interrogatory 3 on pages 7 to 8 of Exhibit 42?

MR. PATTON: Just a second.

Can you read back that question?

BY MR. ABDO:

Q Let me state it more clearly because that's a bit fragmentary.

With respect to upstream surveillance as it operated in 2015, could the term "filtering mechanism" include, quote, the use of a screening device in the upstream Internet collection process to acquire only Internet transactions containing at least one task selector?

MR. PADGETT: I'm sorry, I need to hear that one more time.

(The reporter read back the question.)

MR. PADGETT: I guess I would ask,

before we instruct the witness whether they can answer or not, are you referring to filtering mechanism as used in the document that's referred to by Interrogatory No. 3?

MR. ABDO: Yes.

MR. PADGETT: So can we see?

MR. ABDO: It's one of your briefs from the Fourth Circuit.

MR. PATTON: Let's go off the record.

(Off the record at 3:26 p.m.)

(Resume at 3:38 p.m.)

(The reporter read back the question.)

MR. PATTON: Objection, vague.

You can answer.

THE WITNESS: Okay. So I think the best description for how the process works in the unclassified realm is going to be on page 37 of the PCLOB Report, which is Exhibit 43.

To the extent that the -- so where it says -- the sentence starting, "The provider is compelled to assist the government in acquiring communications across these circuits, to identify

and acquire Internet transactions associated with the Section 702 task selectors on the Internet backbone. Internet transactions are first filtered to eliminate potential domestic transactions, and then are screened to capture only transactions containing a task selector."

Now, my understanding is that there's this other brief that comes up with a new term called "filtering mechanisms"; that's not meant to be something special or otherwise different from the process that was described in PCLOB.

To the extent that you have specifics about the how and the when and the what, that would be classified, but those were not designed to be somehow describing something different.

BY MR. ABDO:

Q Okay. And for the record, you're reading from the top of page 37 of Exhibit 43, correct?

A That is correct.

Q The sentence beginning, "To identify and acquire"?

A That is correct.

Q So would the use of an IP filter fall within the description of that sentence in which it says, "Internet transactions are first filtered to eliminate potential domestic transactions"? Is that where an IP filter could be used?

A Yes, that is an example of where -- an IP filter is an example of something that could be used to do that filter.

Q Okay. And is the use of a screening device described in the NSA's response to Interrogatory 5 in Exhibit 42, is that use of a screening device what could be used to accomplish what is described in the second portion of the sentence that you were reading from page 37 of Exhibit 43, that second part saying, quote, then our screened capture only transactions containing a task selector?

A Yes.

Q Okay. And with respect to upstream surveillance as it operated in 2015, what else could the term -- sorry, what else -- what other

processes could be used to accomplish either the filtering or the screening described in the sentence you were reading from page 37 of Exhibit 43?

MR. PATTON: Objection, calls for classified information, information subject to the statutory privileges.

Instruct the witness not to answer.

THE WITNESS: I will follow the instructions.

BY MR. ABDO:

Q Okay. Are all transactions that were subject to upstream surveillance in June 2015 subjected to Internet protocol filtering --

MR. PATTON: Objection.

BY MR. ABDO:

Q Sorry, let me just finish the question real quick.

-- to eliminate potential domestic transactions from upstream surveillance?

MR. PATTON: Objection, calls for classified information, information subject to the

statutory privileges.

Instruction not to answer the question.

THE WITNESS: I will follow the instructions.

BY MR. ABDO:

Q Can you please describe all the ways in which the NSA could determine in 2015 or could determine today whether a transaction is wholly domestic in order to filter it out from upstream surveillance?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: Could you break that down into 2015 to 2017 to make it clear?

BY MR. ABDO:

Q Could you please describe all the ways in which the NSA could determine in 2015, as part of upstream surveillance, whether a transaction is wholly domestic so as to filter it out?

MR. PATTON: Objection, calls for classified information in order to respond fully

to that question.

There may be an unclassified response to that question, but without knowing what the witness's answer would be, I'm not comfortable just turning that over to her, but I believe there is an unclassified response, but it's also one that she has given you already.

BY MR. ABDO:

Q Okay. If there's nothing more that you could say that's unclassified, let me know that you'll follow your counsel's instruction not to provide any further information.

A There's no additional information that can be provided. What you see here is as much unclassified information as available.

Q And by "here," you're referring to Exhibit 43, page 37?

A Page 37, or the interrogatories.

Q The responses we've been discussing?

A The responses, yeah. There's no additional information to be provided.

Q Okay. What does it mean to say, as

the NSA's response to Interrogatory 3 does, that wholly domestic Internet transactions are, quote, eliminated? And that's in Exhibit 42, I think at page 7 to 8.

MR. PATTON: Object to the extent it calls for classified information and information protected by the statutory privileges.

There is an unclassified answer that the witness can give.

THE WITNESS: So you're asking what does it mean to eliminate?

BY MR. ABDO:

Q Yes.

A So I think if you look at the response, it's important to understand that it starts with -- the sentence is that the devices utilized in the upstream Internet collection process that were designed to eliminate wholly domestic transactions.

So they were -- it's important to recognize it was designed, not that it was actually done.

Q Understood. So let me then be clear.

What does it mean to say -- what were they designed to do in eliminating wholly domestic --

A So that they wouldn't --

Q -- transactions?

MR. PATTON: Same objection, same instruction.

THE WITNESS: They're designed so that they don't make it through to being ingested by NSA's -- into NSA's repository. That's what it means to be designed to eliminate.

BY MR. ABDO:

Q And the repository is what holds communications that contain a selector and are not wholly domestic as of June 2015?

MR. PATTON: Object to the extent it calls for classified information and statutory privileges. You can answer to the extent unclassified.

THE WITNESS: So --

BY MR. ABDO:

Q I'm just trying to understand.

When you say "ingested," you're referring to the databases or the places in which the NSA stores communications that are ultimately authorized by Section 702 to collect?

A Yes, yes. It's when NSA collects it.

MR. PATTON: Same objections.

THE WITNESS: Yes. NSA collects, acquires, ingests. It's the point at which NSA now has it.

BY MR. ABDO:

Q Understood. Can an e-mail address be a selector under upstream surveillance?

A Yes.

Q Can a phone number be a selector under upstream surveillance?

A Yes.

Q Can an Internet protocol address be a selector under upstream surveillance?

MR. PATTON: Objection, calls for classified information and privileged information

pursuant to the statutes aforementioned, and instruct the witness not to answer the question.

THE WITNESS: I will follow the instructions.

BY MR. ABDO:

Q Can a URL, or uniform resource locator, be a selector under upstream surveillance?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

MR. PATTON: Just a moment.

MR. PADGETT: Let's go off the record to discuss.

(Off the record at 3:49 p.m.)

(Resume at 3:53 p.m.)

BY MR. ABDO:

Q We're back from break, and the question was can a URL be a selector under upstream surveillance?

MR. PATTON: Objection, calls for

classified information and information protected by the statutory privileges.

Instruct the witness not to answer.

THE WITNESS: I will not answer.

BY MR. ABDO:

Q Could a URL be a selector under upstream surveillance as of June 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. ABDO:

Q Are the selectors used for upstream surveillance the same as those used for PRISM surveillance as of June 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Wait, I'm sorry. Can you ask the question again?

BY MR. ABDO:

Q Sure. I'll modify it slightly to make it grammatically correct.

Were the selectors used for upstream surveillance the same as those used for PRISM surveillance in June 2015?

MR. PATTON: Same objection, same instructions.

THE WITNESS: Can you just --

MR. ABDO: Ms. Jaques, would you mind marking this as Exhibit -- you're still looking at something for this question?

THE WITNESS: Yes, I am.

The only thing I would state which is definitely not classified is on page 6 of the Civil Liberties and Privacy Office Report, Exhibit 44. At the very top of page 6 it says, "The process for approving the selectors for tasking is the same for both PRISM and upstream collection."

I realize that's not exactly the question you were asking, but I just wanted to make sure you had that piece of information.

BY MR. ABDO:

Q Thank you. Ms. Jaques, would you mind

marking this 46? And it's the entire folder.

(Deposition Exhibit 46 was marked for identification.)

BY MR. ABDO:

Q Ms. Richards --

A Oh, this is fabulous, okay.

Q You have in front of you what's marked as Exhibit 46. Do you recognize that document?

A I do.

Q And what is that document?

A This is the Privacy and Civil Liberties Oversight Board Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, March 19, 2014.

Q Did employees of the NSA testify at that hearing?

A Yes.

Q And they were testifying in their official capacity as NSA employees?

A Yes.

Q Could you turn to page 57 of the

transcript? Do you see at lines 17 to 20 there's a statement that's labeled as coming from Mr. De, spelled D-E?

Do you understand that to be -- who do you understand that to be?

A I'm sorry, we're at line?

Q Lines 17 to 20 of page 57.

A 17 to 20, okay.

Q Of Exhibit 46.

A Mr. De. Oh, let me just --

Q Before getting to the substance of that sentence, which we'll give you a chance to read in a second, do you know who this Mr. De is who is being referred to?

A Yes. He was the general counsel at the time of NSA.

Q And for the record, his full name is Rajesh De?

A Yes.

Q Could you now read those two lines -- those four lines, 17 to 20 on page 57, to yourself?

A (Witness reviewing document.) Okay.

Q What do you understand Mr. De to have been communicating in this first sentence? And the first sentence was, quote, "And it's the same selectors that are used for the PRISM program that are also used for upstream collection."

MR. PATTON: Objection to form, vague.

MR. ABDO: You can answer.

THE WITNESS: I think similar to what I just read to you, the words on the face of it seem accurate.

I'm not sure what you're trying to ask me. Maybe you can help clarify.

BY MR. ABDO:

Q What I'm trying to understand is whether the selectors that are used for PRISM are also used for Upstream collection, and that seems to be on the face of the statement what Mr. De said at the hearing transcribed in Exhibit 46, but I understood you to refuse to answer the question of whether the selectors that are used for the PRISM program are also used for Upstream

collection, so I'm trying to understand what the difference is between my question and this statement.

A I think I need to go -- sorry.

MR. PADGETT: Can I ask a clarifying question? Because it might involve an instruction.

MR. PATTON: Right. There's also a difference of what we're talking about here, so I don't know whether the witness is aware of that, the differences.

MR. ABDO: Are you saying you need to talk in the SCIF?

MR. PATTON: I don't know that we need time to talk in the SCIF, but the objection was to something A, and this is meaning something B, if you know what I mean, and therefore I want to get you that answer because I think that answer is unclassified.

MR. ABDO: Is there an answer that the witness --

MR. PATTON: Because I can understand

why you're having this question, but I'm trying to figure out the best way to get you that unclassified answer.

BY MR. ABDO:

Q Ms. Richards, do you understand the distinction your counsel is drawing between this statement by Mr. De at the hearing transcribed in Exhibit 46 and the question that I asked a few moments ago about whether selectors used for Upstream are the same as those used for PRISM surveillance?

If you know the answer to my question, could you please answer it?

A So let me see if I can restate the two different questions, and maybe I need to have you read back to me what you asked before and we objected to on classified, which is this statement states, "it's the same selectors that are used for the PRISM program that are also used for upstream collection."

A few minutes ago, you had asked whether this was true, and I declined to comment

for classified purposes.

Q Right.

A That's the --

Q Well, let me phrase it this way.

Is the statement that Mr. De made at this hearing in March of 2014 true, or was it true at that time that, quote, it's the same selectors that are used for the PRISM program that are also used for upstream collection?

A I would like to confer in the SCIF before I give you the answer to both of those questions.

MR. PATTON: I just want to seek clarification for the record.

Are you concerned that there's a privilege issue, a classification issue? Is that your concern?

THE WITNESS: Yes.

MR. PATTON: Okay.

THE WITNESS: Not with this sentence.

MR. PATTON: Not with the sentence, but whether or not you can answer --

THE WITNESS: With the other question that was asked.

BY MR. ABDO:

Q I see. If I were to rephrase my previous question to be were the selectors used for PRISM surveillance in June 2015 the same as those used for Upstream surveillance?

MR. PATTON: I have to object to the question as to its vagueness. There is an unclassified answer and there's a classified answer, and --

THE WITNESS: And I'm tripping over which one, so I just need to go --

MR. PATTON: -- and I want to get you the unclassified answer.

MR. ABDO: Okay. Can we take a break and go off the record while you guys confer in the SCIF?

(Off the record at 4:03 p.m.)

(Resume at 4:13 p.m.)

BY MR. ABDO:

Q We're back on the record.

The question we left with, Ms. Richards, was what Mr. De meant in the hearing in March 2014, transcribed in Exhibit 46, when he said, "And it's the same selectors that are used for the PRISM program that are also used for upstream collection."

MR. PATTON: Objection to the extent it calls for classified information and information protected by the statutory privileges.

You can answer to the extent unclassified.

THE WITNESS: Okay. So in looking at page 57, it's important to roll back to roughly around page 55 and understand what they were talking about at this point. And, specifically, I would bring you to -- okay, I'm sorry, go back to 54. Where did the language just go? Okay, I'm sorry, page 56.

So Mr. Wiegmann says, "About that selector, correct."

And then Mr. De says, "It is always focused on that account, so I think the key is,

the misperception that some may have that 'about' collection is somehow about a key word or about the person that may be behind that account.

"But all collections under Section 702, whether it's upstream abouts, which is a subset of upstream, or PRISM is all based on the selectors at issue."

Then we have Ms. Brand says, "Just to follow-up on that because that's a good line of inquiry, just to make sure that everyone understands. So you're saying that if someone is emailing about Rachel Brand or about explosives that would not be a permissible about query under your explanation?"

And Mr. De goes on, and what he's explaining then, when we get down to lines 17 to 20, is the type of selectors is the context for this exchange back and forth, which is then how this is -- in talking about the types of selectors, as opposed to "bomb" or "explosive" or a name, he's explaining that these are the same types of selectors.

That is what's the unclassified fact, and then it's furthered by the sentence I mentioned in the Civil Liberties and Privacy Office Report, as opposed to your question you asked earlier where we said that's classified.

BY MR. ABDO:

Q I think I understand.

A Okay.

Q Moving on a bit.

As of 2015, did the procedures approved by the FISC for upstream surveillance permit the NSA to collect an international HTTP transmission of a website if the text of that website contained a selector?

MR. PATTON: Objection, calls for classified information and information subject to the statutory privileges.

Instruct not to answer the question.

THE WITNESS: I will follow the instruction.

BY MR. ABDO:

Q Okay. Sorry, just one second.

(Deposition Exhibit 47 was marked for identification.)

BY MR. ABDO:

Q Ms. Richards, you have in front of you what's been marked as Exhibit 47.

Do you recognize this document?

A Yes.

Q What is it?

A This is the government's response to the Court's briefing order of May 9th, 2011.

Q With the Court being the Foreign Intelligence Surveillance Court?

A Yes.

Q Do you know which agency of government authored this document?

A It's submitted by the National --

MR. PATTON: Objection to form, vague.

THE WITNESS: -- National Security Division of the Department of Justice, and verified by National Security Agency.

BY MR. ABDO:

Q Okay. When you say "verified," you

mean verified as to the accuracy of the statements within it?

A Yes, to the best of the knowledge of the individual doing it.

Q Would you mind turning to page 30 of Exhibit 47? And I should have mentioned at the outset, Exhibit 47 is Bates stamped NSA-WIKI 237 -- sorry, I may not have the full version in mine. Sorry, NSA-WIKI 234 to 277.

Okay, if you turn to page 30, which is marked NSA-WIKI 266, toward the bottom there's a sentence that begins "this figure," and I'll read it. "This figure was then compared to the total take of Section 702 upstream collection of web activity for the month."

Do you know the context in which this sentence was written in unclassified terms?

A Can you clarify your question? I'm not sure I know what you're asking.

Q Was the context of this sentence an effort to respond to the FISC's inquiry of the NSA about the volume of certain forms of the NSA's

upstream collection?

A Can you repeat?

Q I'll repeat that.

Does this sentence come in a paragraph responding to the FISC's inquiry of the NSA about the volume of certain forms of the NSA's upstream collection activity?

A Yes.

Q And was this sentence explaining how the Department of Justice and the NSA arrived at certain figures it was relaying to the FISC in responding to the question?

A Yes.

Q What does "web activity" mean in the context of Internet communications?

MR. PATTON: Object to the form of the question to the extent it calls for a classified answer or an answer that would be subject to the statutory privileges.

The witness can answer if there's an unclassified answer.

THE WITNESS: I'm going to read this

answer over once more before I give you --

BY MR. ABDO:

Q Please. Maybe I can rephrase the question for you.

A Sure.

Q Do you understand "web activity" to refer to activity of the World Wide Web -- or activity on the World Wide Web?

MR. PATTON: Just a second.

(Counsel conferring.)

MR. PATTON: I'm just going to object to the vagueness.

THE WITNESS: I would refer that to meaning as a way of generally talking about the collection of discrete Internet communications.

BY MR. ABDO:

Q Would you understand it to refer to collection -- let me ask this.

Would Internet web browsing constitute web activity?

MR. PATTON: Objection, calls for classified information to the extent that it's

being asked in the context of upstream collection in this particular document, and subject to that objection and to the statutory privileges that would protect that.

I instruct the witness not to answer the question.

THE WITNESS: I will follow the instruction.

BY MR. ABDO:

Q Do you understand the meaning of the term "web activity" generally, not with regard to this document?

A Yes.

MR. PATTON: Object. Object that it's beyond the scope of the 30(b)(6), but the witness can answer.

BY MR. ABDO:

Q What does it mean generally beyond -- you know, outside of the context of this document, Exhibit 47?

MR. PATTON: Same objection.

THE WITNESS: You say activity on the

Internet?

BY MR. ABDO:

Q Any activity on the Internet. You don't understand "web activity" to be distinct from "Internet activity"?

MR. PATTON: Same objection.

THE WITNESS: I think it's a vague enough term it could be meant any number of different things.

BY MR. ABDO:

Q You don't understand it to mean specifically the protocol referred to as the World Wide Web, which encompasses HTTP and HTTPS communications? That's not how you understand an Internet professional would understand that term?

MR. PATTON: Same objection, adding objection that it calls for expert opinion, and also object that it's asked and answered.

THE WITNESS: I don't think there's a set definition for "web activity." I think it could mean Internet activity, it could mean World Wide Web activity. It could mean any of those

different -- those particular different ones.

I think you have to look at the context for the sentence, and then make a decision accordingly.

BY MR. ABDO:

Q Do you have any reason to believe that this sentence was inaccurate, "this sentence" again in Exhibit 47 beginning, "This figure was then compared"?

A No.

Q Does it disclose classified information?

MR. PATTON: As redacted?

MR. ABDO: As it appears in Exhibit 47.

THE WITNESS: I don't think so.

BY MR. ABDO:

Q To your knowledge, is the term "web activity" ever otherwise used by the NSA in publicly disclosed documents interchangeably with "Internet activity" at large?

MR. PATTON: Object to the form,

vague.

THE WITNESS: I don't know that I've seen "web activity" used in other documents that are unclassified -- that have been declassified. To the extent you're going to show me one next --

BY MR. ABDO:

Q I don't have one. I'm asking.

A So if this is the only instance of this and you're -- you know, I don't have -- I haven't seen it in any of the other documents I've read in the last few weeks, or since we've been prepping for this, so --

Q I'm not trying to play a game of gotcha. I'm asking because your answer suggested that you believe "web activity" to be essentially used interchangeably with the very generic term "Internet traffic" or "Internet communications," and I would assume, if that were the case, then the NSA would in fact use that term interchangeably, but I don't believe that to be the case. I'm asking why that is.

MR. PATTON: Object to the extent it

mischaracterizes prior testimony.

THE WITNESS: I don't have any specific further information that would help elucidate this conversation.

Anything further I might say would go into a classified discussion, and so I can't give you any further explanation as to the use of the word "web" there.

BY MR. ABDO:

Q Under upstream surveillance, as conducted in June 2015, was the NSA permitted to collect the communications of a foreign target with a website in the United States?

MR. PATTON: Just a second.

(Counsel conferring.)

MR. PATTON: Object to the form, vague and ambiguous, and also object that it could call for classified information and information protected by the statutory privileges.

Depending on what the question means, there might be an unclassified answer.

BY MR. ABDO:

Q Do you have an unclassified answer, Ms. Richards?

MR. PATTON: And if she does, I'd like to hear it before she gives it to make sure that it is unclassified.

BY MR. ABDO:

Q Let me give you another question to consider.

A I was just going to say, do you have a whole bunch of them, and then we can go and confer on what those might be?

Q I have one other.

A Okay, but could you repeat that one again?

Q Let me repeat that one, and I'll tell you the other one.

A Yeah.

Q The first one is, under upstream surveillance as approved as of June 2015, was the NSA permitted to collect the communications of a foreign target -- that is, somebody who is a

foreign target of upstream surveillance -- abroad with a website in the United States?

Do you understand my question?

A I do understand.

I don't think there's an unclassified answer, but to the extent --

Q Okay. The second question that I hope you'll consider in the SCIF, under upstream surveillance as it was implemented in June 2015, was the NSA permitted to collect the transactions or communications of a non-targeted foreigner abroad with a website in the United States if the website contained a selector tasked for collection?

A A non-targeted foreigner abroad on a U.S. --

Q With a website in the United States.

A With a website in U.S.

Q If the website contained a selector task for collection. You're generally --

MR. GILLIGAN: I'm baffled by the question.

MR. ABDO: A non-foreign target -- I'm sorry, a non-targeted foreigner abroad communicating with a website in the United States, and the website contains a selector.

MR. GILLIGAN: You mean communicating with a website?

MR. ABDO: Yeah. They visit the website, for example. They're communicating with a website.

MR. GILLIGAN: Yeah, that's what was baffling, what you meant by "with."

MR. ABDO: Communications to and from.

THE WITNESS: So the selector is looking at the website?

BY MR. ABDO:

Q Suppose a non-targeted foreigner abroad is viewing a website, and the website is stored on a web server in the United States, and it contains a task selector --

A The website?

Q The website. And that task selector is being communicated back to this non-targeted

foreigner abroad, and it passes through something being monitored by the NSA in upstream surveillance, did the NSA have the authority in 2015 to collect that communication?

MS. HANLEY COOK: Should we go off the record now?

MR. ABDO: Okay, thanks.

MR. PATTON: Thank you.

(Off the record at 4:30 p.m.)

(Resume at 4:46 p.m.)

MR. PATTON: The witness has reviewed in the interim the applicable targeting procedures, the declassified public version of those, and is prepared to make a statement on that particular point, but we don't believe that anything beyond what she's going to say can be said on the public record.

So to the extent not covered by what she's about to say, we object to the questions to the extent they call for a classified response subject to state secrets and subject to the statutory privileges.

THE WITNESS: The examples you provided are classified. How the targeting might or might not occur is all classified on page 5. It's all black, so we can't go any further into that information.

If you would like to -- I'm sorry. I'm looking at Exhibit A, the procedures used by the National Security Agency for targeting non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978 as amended. These are dated June 2014.

BY MR. ABDO:

Q What page were you looking at of those?

A 5.

Q If I understand, page 5 relates to the NSA's method for assessing whether there would be a foreign intelligence purpose for collecting certain Internet communications, right?

A Yes.

Q My question didn't deal with whether the NSA in fact had reason to or would want to collect Internet communications.

My question was, did the NSA, in June of 2015, have the authority to collect the communications of a foreign target abroad with a website in the United States?

MR. PATTON: The answer to that question is classified and subject to statutory privileges.

Instruct the witness not to answer the question.

THE WITNESS: I'll follow the instructions.

BY MR. ABDO:

Q And under upstream surveillance as conducted in 2015, did the NSA have the authority to collect the transactions of a foreigner abroad with a website in the United States if the website contained a selector task for collection?

MR. PATTON: Same objection, same

instruction.

THE WITNESS: I'll follow the instruction.

BY MR. ABDO:

Q Are you aware that the Office of Director of National Intelligence has acknowledged that there was a time when overcollection of webmail in-boxes had contributed to the -- had occurred under upstream collection?

MR. PATTON: Just a second.

(Counsel conferring.)

THE WITNESS: Can you point to the document or provide whatever that is?

BY MR. ABDO:

Q I'm asking whether you're aware that that's the case.

A I would want to see where exactly ODNI had said that information to make sure that I wasn't somehow going into some sort of classified discussion.

Without the context of what you're saying, as we've seen a few times, sometimes the

information on its face looks like it says one thing, as we just went through with Raj De's back and forth. So without seeing the context of whatever that is, I don't know how to answer.

Q Let me ask a different question then.

Do you know the answer to the question I asked? Well, let me ask that. Do you know the answer to the question I asked?

MR. PATTON: Objection, vague as to which question.

MR. ABDO: The question being whether you're aware that the Office of Director of National Intelligence has acknowledged that one of the overcollection problems that the NSA had with upstream surveillance involved the collection of webmail in-boxes? Do you know the answer to that question?

THE WITNESS: Again, without confirming or denying, I need to see the document you're referring to to better understand. I'm just concerned I'm in classified territory.

BY MR. ABDO:

Q I'm not asking you for an answer to that question. I'm asking whether you know the answer to that question first.

A I'm sorry, I don't know how to answer what you're saying.

MR. GILLIGAN: It's circular. The question is whether she knows, so I don't know whether she knows the answer to that question is the same question.

MR. ABDO: If forced to answer that question, do you know whether you would say yes or no? I'm not asking you to say yes or no, I'm asking whether you know which one you would say if you were forced to answer the question?

THE WITNESS: And so I'm sorry, I don't know what document you're referring to. I assume you're referring to some document somewhere that ODNI published, and if I could see that so that I could look at it, I would be able to tell you whether I know the answer or not.

But in the abstract question of, "Do

you know this?," I can't answer one way or the other. So without sort of having some basis in what we're looking at, I'm having a hard time answering.

BY MR. ABDO:

Q Okay. Was the collection of webmail in-boxes in fact one of the overcollection problems the NSA had with upstream surveillance specifically with regard to multi-communications transactions?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: I just want to state for the record that neither the witness nor I are trying to be difficult here. We are concerned about providing responses to information that we haven't seen, and so I don't want to instruct the witness not to answer the question if there's a public document out there.

I think it would be better if you show it to her. It will either refresh her recollection and she'll be able to explain whether

she's seen it before or anything like that, but at this point, she's not wanting to answer the question, and I'm concerned that the answer may be classified.

MR. ABDO: Are you able to determine whether the answer is classified without knowing whether there's a physical document in the world that contains the information? Is that the definition of "classified"?

MR. PATTON: No, it really gets to, at this particular point, we don't know what it is that you're referring to, and it may be an unclassified document that the Director of National Intelligence has said X, Y or Z. If that's it, it provides the context and some form of comfort for the witness, who is being asked to determine what's on one side of the classified line and what's not on the other.

She signed a Non-Disclosure Agreement and is -- I mean, her responses to you so far have tried to give you as much unclassified information as possible. She's evidently concerned that if

she provides a response to this outside of any context that she might be violating that NDA.

BY MR. ABDO:

Q Are you aware that the Office of Director of National Intelligence, on August 21st of 2013, held a conference call with reporters in which the Office of Director of National Intelligence described the overcollection of webmail in-boxes as an example of the overcollection problem the NSA experienced under upstream surveillance with regard to multi-communication transactions?

MR. PATTON: Again, that may have occurred on August 21st, 2013. It may be a document that is a newspaper article that may or may not be accurately depicting what ODNI said at that time. And so our concern again, in the abstract, is whether or not the information you're providing is both accurate and unclassified.

MR. ABDO: Okay. So can I confirm, at least for the time being, are you instructing the witness not to answer the question?

MR. PATTON: At the moment, I don't think the witness is in a position to answer the question. Factually, I don't know what it is that you're referring to. And given the amount of information that has been provided through unofficial sources, our concern, and my duty here, and the witness's duty, is to protect classified information, and we want to provide as much unclassified information as we can --

MR. ABDO: I understand. I'm just asking a simple question, Rodney. Are you instructing the witness not to answer?

MR. GILLIGAN: Tell you what, if we step outside, I might be able to suggest a way around this.

MR. ABDO: Can we go off the record?

(Off the record at 4:57 p.m.)

(Resume 5:04 p.m.)

THE WITNESS: Is there an outstanding question? Where are we?

BY MR. ABDO:

Q There was. Let me start with the

question outstanding, which was are you aware that the Office of Director of National Intelligence has acknowledged that the NSA has collected webmail in-boxes under upstream surveillance?

MR. PATTON: Object to the form as beyond the scope of the 30(b)(6) notice, and the witness can answer in her personal capacity.

THE WITNESS: I'm not aware.

BY MR. ABDO:

Q Has the NSA collected webmail in-boxes as part of upstream surveillance?

MR. PATTON: Object to the question, calls for classified information and information protected by the statutory privileges, and instruct the witness not to answer the question.

THE WITNESS: I will follow the instructions.

BY MR. ABDO:

Q Okay. Are you familiar with the fact that the contents of Internet communications are transported in what is known as the application layer of Internet packets?

MR. PATTON: Object to the question to the extent it calls for classified -- I'm sorry, I'm so used to that -- to the extent it calls for expert opinion, and that it's beyond the scope of 30(b)(6).

THE WITNESS: Yes.

BY MR. ABDO:

Q Okay. Are you aware of the fact that the contents of an email communication are transported within the application layer of Internet packets?

MR. PATTON: Same objections.

THE WITNESS: Yes.

Isn't that what you just asked me?

BY MR. ABDO:

Q The first question was with respect to Internet communications generally, and the second question was with respect to email communications specifically.

A Okay.

Q Is your answer to both yes?

A Yes. It sounded like the same one,

and I worried I was missing something.

Q And are you aware of the fact that the contents of a website are transported within the application layer of Internet packets?

MR. PATTON: Same objections.

THE WITNESS: Yes.

BY MR. ABDO:

Q Are the filtering or screening processes that you've described with respect to upstream collection as it operates -- or excuse me, upstream surveillance as it operated in June 2015 -- forms of deep packet inspection?

MR. PATTON: Objection.

(Counsel conferring.)

MR. PATTON: I'm sorry, could you read that back?

BY MR. ABDO:

Q Sure. Are the filtering or screening processes that you've described under upstream surveillance as conducted in June 2015 forms of deep packet inspection?

MR. PADGETT: I'm sorry, one key thing

I didn't get. Could you read that back?

(The reporter read back the question.)

MR. PATTON: Object to the question because it calls for classified information and information protected by the statutory privileges.

Instruct the witness not to answer.

THE WITNESS: I will follow the instructions.

BY MR. ABDO:

Q Are you familiar with the term "deep packet inspection"?

MR. PATTON: Object to that question, beyond the scope of 30(b)(6), and it calls for an expert opinion.

THE WITNESS: In the general sense of the word, as in not specific to anything in particular, but known as the outside world?

BY MR. ABDO:

Q Not specific to upstream surveillance, but --

A Yes.

Q You are familiar with it?

A Yes.
Q What does it mean?
MR. PATTON: Same objections.
THE WITNESS: It's the concept of -- I'm sorry, I'm --
BY MR. ABDO:
Q Is it the process of examining or analyzing the application layer of packets traversing the network?
MR. PATTON: Same objections.
THE WITNESS: Yeah, I'm -- yes. Yes, that's a fine description.
BY MR. ABDO:
Q Tell me again your position at the Department of Homeland Security.
A I was the Senior Director for Privacy Compliance in the Privacy Office.
Q And you participated in the drafting of Privacy Impact Assessments?
A I did.
Q Were you involved in the Privacy Impact Assessments conducted for the Einstein 2 or

Einstein 3 programs?

A Yes, which is why I changed the answer when you asked about the four types of sort of --

Q Ah, got it.

A When I rechanged it, I realized that would probably constitute what you were considering to be surveillance.

Q Network surveillance?

A Network surveillance.

Q Did Einstein 2 involve deep packet inspection?

A I honestly don't remember.

MR. PATTON: Just object to that question as beyond the scope of 30(b)(6). I'm not sure whether the answer is unclassified or not since I have not consulted with the Department of Homeland Security, but if the witness knows of an unclassified answer, the witness can give an unclassified answer.

BY MR. ABDO:

Q Sorry, please go ahead.

A I apologize, but I don't remember what

is classified or unclassified about the Einstein 2 PIA, so unless you have a copy of what was published, I can't speak to the specifics of what was in it.

Q Okay. Are you familiar with Einstein 3? Generally, not anything specific, but are you aware of the Department of Homeland Security's intrusion detection and intrusion prevention program known as Einstein 3 Accelerated?

MR. PATTON: Objection to beyond the scope of 30(b)(6), potentially classified. I'll have to rely on the witness, who may be more familiar with the DHS program certainly than me. If there's a unclassified answer, you can give it in your personal capacity.

MR. ABDO: Surely the existence of this program is unclassified, but --

MR. PATTON: I'm not willing to take the risk.

BY MR. ABDO:

Q Did you work on the Privacy Impact

Assessment for Einstein 3?

MR. PATTON: Same set of objections.

THE WITNESS: Generally speaking, yes, because every PIA that was approved by the Department of Homeland Security at that point was reviewed by me.

BY MR. ABDO:

Q Okay. Are you aware that Einstein 3 was part of the comprehensive cybersecurity initiative announced by the Obama administration?

A Yes.

MR. PATTON: Same objections.

THE WITNESS: Oh, sorry.

BY MR. ABDO:

Q And are you aware that, in announcing that, the administration also made clear that Einstein 3 was implemented with the technological support of the NSA?

MR. PATTON: Same objections.

THE WITNESS: Do you have a document that provides that information?

MR. ABDO: Sure.

(Deposition Exhibit 48 was marked for identification.)

BY MR. ABDO:

Q You have what's been marked as Exhibit 48 in front of you, Ms. Richards.

Do you recognize this document?

MR. PATTON: Object to this document as beyond the scope of 30(b)(6), but the witness can answer this and any other series of questions you have that have unclassified answers and are within her personal knowledge.

THE WITNESS: Yes, I've seen this document before. It's been quite some time.

BY MR. ABDO:

Q Can you tell us what it is?

A It's the Comprehensive National Cybersecurity Initiative.

There it is. Look at that.

Q Would you turn to page 3 of it, about halfway down, two-thirds of the way down, the sentence beginning, "DHS is currently conducting a[n] exercise" -- I think they meant an

exercise -- "to pilot the EINSTEIN 3 capabilities described in this initiative based on technology developed by NSA to solidify processes for managing and protecting information gleaned from observed cyber intrusions."

A Yes.

Q So is it true that the Einstein 3 program was piloted based on technology developed by the NSA?

MR. PATTON: Just a moment.

(Counsel conferring.)

THE WITNESS: Do you have the date of this document?

BY MR. ABDO:

Q I believe it's 2010, but I don't know off the top of my head.

A Could I see your Einstein 3 PIA?

Q We've got another copy of it. Can we mark this too, Dawn?

(Deposition Exhibit 49 was marked for identification.)

BY MR. ABDO:

Q So just for the record, you're now looking at what's been marked as Exhibit 49.

Do you recognize that?

A Yes.

Q What is that document?

A The Privacy Impact Assessment for the National Protection and Programs Directorate, Department of Homeland Security, Einstein 3 Accelerated (E3A), dated April 19th, 2013.

Q Okay. And for the record, you participated in the drafting of that assessment?

A I reviewed it.

Q Okay. If you're not quickly familiar with the answer to a question, that's fine, we can move on. I was just asking whether the Comprehensive National Cybersecurity Initiative --

A So my answer to you --

MR. PATTON: Just a second.

THE WITNESS: I'm sorry.

MR. PATTON: Just preserving my objection that both Exhibit 48 and Exhibit 49,

that series of questions are outside the scope of 30(b)(6), and the witness is answering in her personal capacity.

THE WITNESS: To the extent that the CNCI information is from 2010, stating something specific about NSA-developed technology, and not having reviewed this in almost five years, I would have to look at those and really understand whether what was described in 2010 actually got implemented in 2013.

MR. ABDO: Understood. Okay.

MR. GILLIGAN: Sorry, is that 49 there?

MR. ABDO: 49, yeah.

THE WITNESS: I can read it if you would like me to, but --

BY MR. ABDO:

Q No, that's okay.

Is it correct that in upstream collection that NSA obtains what it calls transactions?

A Internet transactions.

Q Internet transactions. Sorry, yes, internet transactions.

A Yes.

Q Do the Internet packets that constitute a single Internet transaction have a common destination?

MR. PATTON: Objection. Just a second.

(Counsel conferring.)

MR. PATTON: We're just trying to see if there's an unclassified response to that.

THE WITNESS: Uh-uh.

MR. PATTON: Objection, calls for a classified response and information subject to the statutory privileges.

Instruct the witness not to answer.

THE WITNESS: Instructions will be followed.

BY MR. ABDO:

Q Okay. Do the Internet packets that constitute a single Internet transaction have a common source?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instructions.

BY MR. ABDO:

Q Are you familiar with the term "flow" or "network flow" as used in the context of Internet communications?

MR. PATTON: Objection, it's beyond the scope of 30(b)(6), and it's calling for an expert opinion.

THE WITNESS: I am, but don't make me define them.

BY MR. ABDO:

Q Is an Internet transaction, as understood by the NSA, the same as a flow or network flow as used in the context of Internet communications?

MR. PATTON: Just a moment. I don't think she can answer that.

THE WITNESS: Uh-uh, no. No, I can't answer that.

(Counsel conferring.)

MR. PATTON: Same objection, same instruction.

THE WITNESS: And will follow the instruction.

BY MR. ABDO:

Q And the reason you can't answer is because it would disclose classified information?

A No.

Q Not because you're not familiar with the definition of "flow"?

A No, not because -- no, that is correct. I know what flow is, I just don't -- that's classified.

Q Okay. Is the definition of "flow" classified?

MR. PATTON: Objection, beyond the scope.

BY MR. ABDO:

Q In general as that term is commonly used in the network communications industry?

MR. PATTON: Objection, it's beyond

the scope, and calling for telecommunications expert opinion.

THE WITNESS: As you've just described, it's the general meaning. There's no specific definition. Internet transaction is an NSA definition. It's not a commonly understood telecommunications one.

So it, like -- there was one another we had earlier today. So there's sort of different groups of NSA-specific versus the outside world would know what they are. "Internet transaction" is one of those.

BY MR. ABDO:

Q What about network flow, flow or network flow?

A Those would be the normal everyday use of the words.

Q In other words, the NSA doesn't have a special definition of that term?

A Correct.

Q Okay. Can we take a five-minute break?

MR. PATTON: Sure.

(A break was taken at 5:21 p.m.)

(Resume at 5:35 p.m.)

EXAMINATION BY COUNSEL FOR

WIKIMEDIA FOUNDATION AND THE ACLU

BY MR. TOOMEY:

Q Ms. Richards, so I'm going to be asking some --

MR. ABDO: Why don't you introduce yourself.

BY MR. TOOMEY:

Q I'm Patrick Toomey. I'm counsel for Wikimedia Foundation from the American Civil Liberties Union.

So carrying on, in the course of upstream surveillance, does the NSA review the contents of communications as they are in transit on the Internet backbone?

MR. PATTON: Objection, calls for information that's classified, subject to state secrets, and the other statutory privileges.

Instruct the witness not to answer.

THE WITNESS: I will follow the instructions.

BY MR. TOOMEY:

Q Let's focus on the period of June 2015 for the questions that follow.

In the course of upstream surveillance in June 2015, did the NSA review the contents of communications as they were in transit on the Internet backbone?

MR. PATTON: Same objections, same instructions.

THE WITNESS: Will follow the -- oh.

MR. PATTON: There are unclassified facts that could come out with different questions, but for that particular phrasing, instruct her not to answer.

THE WITNESS: Will follow the instructions.

BY MR. TOOMEY:

Q In the course of upstream surveillance in June 2015, did the NSA scan the contents of communications as they were in transit on the

Internet backbone?

MR. PATTON: Let me just confer, because there's a specific phrase that you're using that I think is causing both NSA counsel and I as a basis to object on classified information. So I don't want to appear we're overclassifying Einstein 3.

MR. GILLIGAN: So we can go off the record.

MR. TOOMEY: Let's go off the record for a minute.

(Off the record at 5:37 p.m.)

(Resume at 6:23 p.m.)

MR. PATTON: Can remind us of where we were?

MR. TOOMEY: Yes. We're going back on the record, and, Ms. Jaques, if you could read back the previous question, please.

(The reporter read back the question.)

MR. PATTON: Objection to the question to the extent it calls for classified information and information protected by the statutory

privileges. The witness can answer the question to the extent unclassified.

THE WITNESS: So I think what you're asking is sort of a two-part question, and so I wanted to unpack and provide the unclassified aspects of it, and then sort of acknowledge that we've got the classified.

So as part of the upstream, we scan the content of the Internet transactions, and we did that in 2015.

As to the question of basically the in transit or the location, that piece is classified.

BY MR. TOOMEY:

Q Thank you. In June of 2015, in the course of upstream surveillance, did the NSA scan the application layer data of communications that transit the Internet backbone?

MR. PATTON: I'm just listening to your question. There's a slight difference in that that I just need to consult.

(Counsel conferring.)

MR. PADGETT: Could you read the

question?

(The reporter read back the question.)

THE WITNESS: It's classified.

MR. PATTON: There's something unclassified.

MR. PADGETT: Can we just go off the record for a second?

(Off the record at 6:26 p.m.)

(Resume at 6:28 p.m.)

MR. PATTON: And there may be a lot of these back and forth on this, so ...

THE WITNESS: Can you repeat the question, please?

(The reporter read back the question.)

MR. PATTON: Objection to the extent it calls for classified information or information protected by the statutory privileges.

The witness can answer to the extent unclassified about June 2015.

THE WITNESS: So to make sure I'm accurately -- I want to make sure I'm understanding the question and making the

distinction.

So what you're saying is what I just said was part of upstream in 2015, we scanned the content of Internet transactions.

Your next question is are we -- is NSA scanning the application layer of the Internet -- of the Internet -- that doesn't make sense -- if we're scanning the Internet -- I'm sorry, the application layer?

BY MR. TOOMEY:

Q Yes. The question is, in June 2015, did the NSA scan the application layer data of communications that transit the Internet backbone?

MR. PATTON: Same objection, same instruction.

THE WITNESS: The answer is yes for 2015, that we scan certain application data of communications that transit the Internet backbone.

BY MR. TOOMEY:

Q When you say certain --

A Mm-hmm, that's important.

Q -- application layer data, what you

mean by "certain"?

MR. PATTON: Objection, misstates prior testimony. Same objections as before, same instruction.

THE WITNESS: I can't go any further. It's classified.

BY MR. TOOMEY:

Q In unclassified terms, in June 2015, how did the NSA determine whether an Internet transaction contained a selector?

MR. PATTON: Object to the extent it calls for -- the whole answer would be classified. The witness can answer to the extent unclassified.

THE WITNESS: I just want to refer to see if there's any additional information I can provide to you beyond what we've already given to you.

There's no additional information beyond what was provided in the Interrogatories 3, 4 and 5, so there's no additional unclassified information beyond the fact that that's conducted.

BY MR. TOOMEY:

Q Is there any classified information that would be responsive to that question?

A Yes. This is necessarily incomplete because of the classified nature of the program.

Q And you're --

MR. PATTON: We're still talking about June 2015?

MR. TOOMEY: That's correct, yes.

THE WITNESS: Still June 2015, yes.

BY MR. TOOMEY:

Q And you're refusing to provide that information on the basis of an instruction from your lawyer?

MR. PATTON: I haven't instructed her on that, but her answer did indicate what was unclassified, which was the interrogatory responses to 3, 4 and 5, I believe she said, and I believe she also said that anything else beyond that was classified.

And there wasn't a pending question, but to the extent that you asked her a question

such as tell me what that classified information is, I would instruct her not to answer.

BY MR. TOOMEY:

Q Understood. Thank you.

Today does the NSA scan the application layer data of communications that transit the Internet backbone?

MR. PATTON: Objection, calls for information that's classified, subject to the statutory privileges before mentioned, and instruct the witness not to answer.

THE WITNESS: I follow those instructions.

BY MR. TOOMEY:

Q In June of 2015, if a transaction was scanned by the NSA in the course of upstream surveillance, and the NSA determined that it did not contain a selector, was the communication eliminated?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PADGETT: Can you read the

question back?

(The reporter read back the question.)

MR. PATTON: Can we just go off the record for a second?

MR. TOOMEY: Can we go off the record?

(Off the record at 6:34 p.m.)

(Resume at 6:37 p.m.)

(The reporter read back the question.)

MR. PATTON: Object to that question to the extent it calls for classified information or otherwise privileged information.

The witness can answer to the extent unclassified.

THE WITNESS: So the process by which Internet transaction is filtered, and then scanned, if it doesn't have a test selector or isn't about the target, then that means that information will not be ingested into the NSA repository.

BY MR. TOOMEY:

Q And is that communication eliminated?

MR. PATTON: Objection. The question

calls for a classified answer, as well as an unclassified one, which the witness has already given.

The witness can answer again and provide the unclassified answer.

THE WITNESS: I have nothing additional beyond. If you'd like me to repeat what I said, I'd be happy to.

BY MR. TOOMEY:

Q No need to repeat.

And to the extent there is -- is there classified information that you are not providing in response?

A Yes.

Q Today, does the NSA seek to acquire email communications to and from its targets using upstream surveillance?

MR. PATTON: Object to the question. It calls for classified information and information protected by the statutory privileges.

I instruct the witness not to answer.

THE WITNESS: I will follow

instructions.

BY MR. TOOMEY:

Q Could you please describe as fully as possible how, in June 2015, the NSA determined whether an Internet transaction contained a selector?

MR. PATTON: Objection to the extent it calls for classified information, or information otherwise protected by the statutory privileges.

The witness can answer if she can regarding the unclassified response to that question.

THE WITNESS: There's no additional unclassified information beyond what I've already said.

BY MR. TOOMEY:

Q Thank you. Beyond what you've already said or what appears in the NSA's discovery responses, could you please describe as fully as possible how the NSA today determines whether an Internet transaction contains a selector?

MR. PATTON: Objection. The question calls for classified information and information protected by the statutory privileges, and instruct the witness not to answer.

THE WITNESS: I will --

MR. ABDO: Rodney, can we just try to compress if it's the same objection? Thanks.

MR. PATTON: If you ask the same -- exactly those kind of questions, I will do my best. Thank you.

THE WITNESS: I will follow the instructions.

BY MR. TOOMEY:

Q In the course of upstream surveillance in June 2015, did the NSA scan communications in bulk?

MR. PATTON: Objection, calls for classified information. Just check and see if there's a --

(Counsel conferring.)

MR. PATTON: Just a second. Can we go off the record?

(Off the record at 6:40 p.m.)

(Resume at 6:43 p.m.)

MR. TOOMEY: Can you please repeat the question?

(The reporter read back the question.)

MR. PATTON: Objection. We'd need to go into the SCIF to discuss whether or not there's an unclassified response to this.

THE WITNESS: But before we do that, can you give a definition of what you mean by "bulk," scanning communications in bulk?

BY MR. TOOMEY:

Q Does the NSA ever use the term "bulk" in connection with surveillance activities?

A Yes.

Q And what do you understand the NSA to mean by the term "bulk"?

A To do collection without -- let's see, the definition is in Presidential Policy Directive No. 28, which I don't have with me, but it's something roughly along the lines of collection without discriminates.

Q That document describes bulk collection to the best of your recollection?

A Yeah.

Q Yes?

A Or it has a general description of it, and then carries on to provide when NSA can conduct bulk -- for what purposes the information can be used.

Q And so my question here is about whether in June 2015, in the course of upstream surveillance, the NSA scanned communications in bulk?

MR. PATTON: Go off the record.

(Off the record at 6:45 p.m.)

(Resume at 6:57 p.m.)

(The reporter read back the question.)

MR. PATTON: Objection to the extent it calls for classified information and information protected by the statutory privileges.

Instruct the witness to answer the question to the extent able in unclassified terms.

THE WITNESS: So in terms of

unclassified, the best information I can give to you is in the PCLOB report, which is Deposition Exhibit 43, page 103. The last line of the first paragraph that states the program does not operate by collecting communications in bulk.

BY MR. TOOMEY:

Q Could you please answer my question about whether in June 2015 the NSA scanned communications in bulk?

MR. PATTON: Objection. The answer to that question, to the extent not already provided by the witness, is classified and subject to statutory privileges.

Instruct the witness not to answer.

MR. GILLIGAN: And state secrets. Did you say state secrets?

MR. PATTON: I said classified. I'm trying to shorten it.

MR. GILLIGAN: Oh, okay. We're all for that.

MR. PATTON: Also subject to the state secrets privilege.

THE WITNESS: I will follow the instructions of my counsel.

BY MR. TOOMEY:

Q In the context of upstream surveillance, is scanning a communication different from collecting a communication?

A Yes.

Q In the course of upstream surveillance today, does the NSA scan communications in bulk?

MR. PATTON: Objection. The question calls for information that's classified, subject to the state secrets, and to the statutory privileges. Instruct the witness not to answer.

THE WITNESS: I will not answer.

BY MR. TOOMEY:

Q In the course of upstream surveillance today, does the NSA scan the metadata of communications in bulk?

MR. PATTON: Same objections, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q In the course of upstream surveillance in 2015, did the NSA copy communications in bulk?

MR. PATTON: Same objection, same instructions.

THE WITNESS: Follow instructions.

BY MR. TOOMEY:

Q In the course of upstream surveillance today, does the NSA copy communications in bulk?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Follow the instructions.

BY MR. TOOMEY:

Q In the course of upstream surveillance in June of 2015, did the NSA deliberately attempt to filter out any of Wikimedia's international communications?

MR. PATTON: Objection. Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q In the course of upstream surveillance today, does the NSA deliberately attempt to filter out any of Wikimedia's international communications?

MR. PATTON: Same instruction, same objections.

THE WITNESS: Will follow instruction.

BY MR. TOOMEY:

Q In the course of upstream surveillance in June of 2015, did the NSA deliberately attempt to filter out all of Wikimedia's communications?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow instruction.

BY MR. TOOMEY:

Q In the course of upstream surveillance today, does the NSA deliberately attempt to filter out all Wikimedia communications?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow

instructions.

BY MR. TOOMEY:

Q Does the NSA contend as a factual matter in this case that it deliberately filters out all Wikimedia communications?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: Could you go off the record?

(Off the record at 7:01 p.m.)

(Resume at 7:08 p.m.)

MR. TOOMEY: Could you read back the last question?

(The reporter read back the question.)

MR. PATTON: Object to the question as beyond the scope of 30(b)(6), improper 30(b)(6) question. The witness can answer in her personal capacity.

THE WITNESS: In my personal capacity, I have no idea, but to the extent that we do or do not filter something out would be classified in any event.

BY MR. TOOMEY:

Q Does anyone at the NSA know whether the NSA contends in this case, as a factual matter, that it deliberately filters out all Wikimedia communications?

MR. PATTON: Same objections, same instruction.

THE WITNESS: It's classified. I mean --

MR. PATTON: That's not the question he's asking.

THE WITNESS: That's not the question.

MR. PATTON: That's not the question he's asking.

THE WITNESS: So same answer, which I have no idea, and to the extent it is or isn't would be classified.

BY MR. TOOMEY:

Q To the extent it is or isn't what?

A Filtering out Wikimedia, as you were contending in your question.

Q My question is whether the NSA

contends that it is filtering out Wikimedia's communications. Do you know the answer to that question?

MR. PATTON: Objection. Same objections as before, and adding asked and answered.

THE WITNESS: I have nothing else to say on the topic.

MR. TOOMEY: Ms. Jaques, could you mark as the next exhibit this document, please?

(Deposition Exhibit 50 was marked for identification.)

BY MR. TOOMEY:

Q So the court reporter has handed Ms. Richards Exhibit 50, which is titled Memorandum of Points and Authorities in Support of Defendant's Motion to Compel Discovery. Sorry, we don't have as many copies of this one, sorry.

Could you please tell me what this document is?

MR. PATTON: Objection, lacks foundation.

BY MR. TOOMEY:

Q You can answer.

Have you seen this document before?

A I have not seen this document before.

Q Can you read the title of the document, please?

A Sure. Memorandum of Points and Authorities in Support of Defendant's Motion to Compel Discovery, dated March 26, 2018.

Q Thank you. Could you please turn to page 11 --

A Sure.

Q -- of Exhibit 50?

I'm going to read a sentence from the document in the last paragraph toward the bottom of the page.

"An entity seeking to conduct surveillance on the Internet that lacks the ability to decipher encrypted HTTPS communications may well decide to program its surveillance equipment to disregard such communications altogether."

Has the NSA programmed its surveillance equipment to disregard HTTPS communications altogether?

MR. PATTON: Objection, the question calls for classified information protected by the state secrets privilege and information protected by the statutory privileges.

Instruct the witness not to answer the question.

THE WITNESS: I'll follow the instructions.

BY MR. TOOMEY:

Q Can we now turn to page 12 of Exhibit 50. I'm going to read a passage from the first paragraph toward the top of the page.

"If the NSA lacked the ability to decipher HTTPS communications," dot dot dot, "then nothing --

MR. PATTON: It's an important dot dot dot.

MR. TOOMEY: We'll get there. I'm going to start again. I'm going to read the

passage again.

"If the NSA lacked the ability to decipher HTTPS communications ... then nothing in the 'technical rules of how the Internet works' ... would prevent the configuration of devices used in connection with Upstream surveillance to exclude HTTPS communications."

Does the NSA have the ability to decipher HTTPS communications?

MR. PATTON: Objection, outside the scope of 30(b)(6), and the question calls for classified information protected by the state secrets privilege, statutory privileges.

Instruct the witness not to answer.

THE WITNESS: I will follow the instructions.

BY MR. TOOMEY:

Q I'm going to read a passage now from page 12 of Exhibit 50 in the second paragraph toward the bottom of the page.

"If the NSA deemed communications to and from Wikimedia's websites to be of low

foreign-intelligence value, then nothing in the technical rules of the Internet would prevent the configuration of equipment used in connection with Upstream surveillance to ignore all communications having source or destination IP addresses associated with Wikimedia."

Has the NSA configured its surveillance equipment to ignore all communications having source or destination IP addresses associated with Wikimedia?

MR. PATTON: Objection, beyond the scope of 30(b)(6), and objection, it calls for classified information, subject to state secrets, statutory privileges.

Instruct the witness not to answer.

THE WITNESS: Will follow the instructions.

BY MR. TOOMEY:

Q Does the NSA deem communications to and from Wikimedia's websites to be of low foreign intelligence value?

MR. PATTON: Same objection, same

instruction.

THE WITNESS: Will follow instruction.

BY MR. TOOMEY:

Q Would the NSA be permitted under upstream surveillance today to collect a targets communications with a U.S.-based website?

A How is this question different than the last one?

MR. PATTON: I'm not sure it is.

THE WITNESS: Okay.

MR. PATTON: Can we go off the record?

(Off the record at 7:16 p.m.)

(Resume at 7:23 p.m.)

BY MR. TOOMEY:

Q Back on the record.

Ms. Jaques, could you please read back the prior question?

(The reporter read back the question.)

MR. PATTON: We object to that question. It calls for a classified answer.

The witness has reviewed during the break the currently applicable declassified and

public targeting procedures, and there's no unclassified answer we can give. So as a result, we object to the question, it calls for classified information, subject to the state secrets and subject to the statutory privileges, and instruct the witness not to answer.

THE WITNESS: I'll follow the instructions.

BY MR. TOOMEY:

Q Is it possible that a targets communications with Wikimedia could contain foreign intelligence information that would be of interest to the NSA?

(Counsel conferring.)

MR. PATTON: You'll like this one.

Object as beyond the scope of 30(b)(6) and speculative. The witness can answer in her own capacity to the extent the answer is unclassified.

THE WITNESS: It's speculative. I can't speak to who would or wouldn't be, what particular individual might be targeted. If an

analyst decides a particular selector or person meets the targeting standards, then that would be appropriate.

BY MR. TOOMEY:

Q Could the term "foreign intelligence information" encompass information that a person surveilled using upstream surveillance is reading on one of Wikimedia's websites?

MR. PADGETT: Could I get that read back?

(The reporter read back the question.)

MR. PADGETT: Do you want to talk about it? Let's go off the record.

(Off the record at 7:26 p.m.)

(Resume at 7:28 p.m.)

MR. TOOMEY: Ms. Jaques, could you please read back the last question?

(The reporter read back the question.)

MR. PATTON: Objection, beyond the scope of 30(b)(6), speculative, and calls for legal conclusion. The witness can answer in her personal capacity.

THE WITNESS: I'm sorry, can you read that question one more time?

(The reporter read back the question.)

MR. PATTON: Same objections.

THE WITNESS: Can we go off the record? Sorry.

(Off the record at 7:30 p.m.)

(Resume at 7:32 p.m.)

MR. PATTON: Same objections, same instruction.

THE WITNESS: So you have a couple of different things, which is why we kept having to walk outside to unpack that, and so I want to unpack what's classified and what's unclassified.

So the first part of your question would be is there possibly foreign intelligence information on the Wikimedia sites, to which the answer, from my perspective, is there could be. I don't actually know. I haven't trolled through the Wikimedia websites, but it's possible.

The second part of that question had to do with how it would function in the upstream

context, and that piece of it is what's classified.

BY MR. TOOMEY:

Q Similar question, could the term "foreign intelligence information" encompass information that a person surveilled using upstream surveillance is contributing to one of Wikimedia's websites?

MR. PATTON: Same objections, same instruction.

THE WITNESS: I would give the same answer, which is I would separate those two pieces to say it's possible that somebody at one of your contributors is creating foreign intelligence information in a hypothetical. I don't actually know.

To the extent it has anything to do with upstream, any piece of that would be classified.

BY MR. TOOMEY:

Q And you're not answering that portion to that aspect of the question based on your

lawyer's instruction?

A Correct.

MR. PATTON: Not based on my instruction. When we broke the last time, the witness had a question as to what aspect of this that she could talk about. She provided the information that she could talk about and indicated to you there's another classified component, and the nature of that classified information, and she declined to answer based on that.

Had you asked her a follow-up question as to the content of that classified information, I would have instructed her not to answer.

BY MR. TOOMEY:

Q Could you please provide any classified information that you believe my question calls for?

MR. PATTON: I respect that question. It keeps our record clean.

Object to the question to the extent it calls for classified information, information

subject to the statutory privileges, and instruct the witness not to answer.

THE WITNESS: I will follow those instructions.

BY MR. TOOMEY:

Q Today, does the NSA intentionally attempt to filter out all HTTPS communications from upstream surveillance?

MR. PATTON: Objection, the question calls for classified information, subject to the state secrets and to the statutory privileges.

Instruct not to answer.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q Same question, but for June 2015. Did the NSA at that time intentionally attempt to filter out all HTTPS communications from upstream surveillance?

MR. PATTON: Same objections, same instruction.

THE WITNESS: Will follow the

instruction.

BY MR. TOOMEY:

Q Today, does the NSA intentionally attempt to filter out all Internet communications that use TCP port 443?

MR. PATTON: Same objections, same instruction.

THE WITNESS: Follow the instruction.

BY MR. TOOMEY:

Q In June 2015, did the NSA intentionally attempt to filter out all Internet communications that used TCP port 443?

MR. PATTON: Same objections, same instruction.

THE WITNESS: Follow the instruction.

BY MR. TOOMEY:

Q Today, does the NSA intentionally filter out all encrypted VPN communications?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q In June 2015, did the NSA intentionally filter out all encrypted VPN communications?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Follow the instruction.

BY MR. TOOMEY:

Q Today, does the NSA intentionally filter out all open VPN communications?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Follow the instruction.

BY MR. TOOMEY:

Q In June 2015, did the NSA intentionally filter out all open VPN communications?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q Today does the NSA intentionally filter out Wikimedia's encrypted VPN communications?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q In June 2015, did the NSA intentionally filter out Wikimedia's encrypted VPN communications?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q Can you please describe in as much detail as necessary to provide a complete answer how the NSA implemented any changes to "about" collection during or after April 2017?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: Object to the question to the extent it calls for classified information and information protected by the statutory privileges.

If there is an unclassified response, the witness can provide it.

MR. TOOMEY: Rodney, to be clear, just so we can try to consolidate things, are you also instructing the witness not to provide any unclassified information?

MR. PATTON: No. I'm instructing --

MR. TOOMEY: Sorry, any classified information, just so --

MR. PATTON: I would love her to provide any unclassified information, but if there's any classified information, I'm instructing her not to answer.

There may be some unclassified information that she can provide, and that's what I'm authorizing her to do.

THE WITNESS: As of 2017, April 2017, NSA changed the way it did its upstream collection

so that it no longer collected the "abouts" collection.

There's not any additional information beyond the information that was either in the 2017 opinion or our associated unclassified information that NSA put out on its website.

MR. PATTON: That's the April 2017 FISC opinion?

THE WITNESS: Sorry, yes, the April 2017 FISC opinion.

BY MR. TOOMEY:

Q Besides the information you just identified, is there any other unclassified information that you could provide to this question?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Not that I'm aware of.

BY MR. TOOMEY:

Q Is there classified information that would answer the question that you are not providing at the instruction of your attorney?

MR. PATTON: Objection to the extent it calls for classified information.

If the witness's answer is yes or no, she can provide that information.

THE WITNESS: Yes.

BY MR. TOOMEY:

Q Apart from the information you identified in response to my last question, could you please describe how the NSA attempts to avoid collecting communications that are solely about a selector?

MR. PATTON: Object to the form of the question, vague as to time. Potentially classified.

(Counsel conferring.)

MR. PATTON: Would you mind rephrasing to specify the time period?

MR. TOOMEY: Sure, I'll rephrase.

MR. PATTON: Thanks.

BY MR. TOOMEY:

Q Apart from the unclassified information that you provided in response to my

last question, could you please describe in as much detail as necessary to provide a complete answer how, after April 2017, the NSA attempts to avoid collecting communications that are solely about a selector?

(Counsel conferring.)

MR. PATTON: Can we go off the record?

(Off the record at 7:42 p.m.)

(Resume at 7:43 p.m.)

MR. PATTON: Would you mind reading back the question, please?

(The reporter read back the question.)

MR. PATTON: Object to the question to the extent it calls for classified information.

If the witness's answer is yes or no, she can answer that.

THE WITNESS: There's no additional information beyond what I've pointed to. I have no additional --

BY MR. TOOMEY:

Q There's no additional unclassified information?

A No additional unclassified information.

Q And is there classified information that you're not providing at the instruction of your counsel?

A Yes.

Q Apart from the unclassified information that you provided in response to my question, my previous question, please describe in as much detail as necessary to provide a complete answer how the change in April 2017 affected the filtering of communications subject to upstream surveillance?

(Counsel conferring.)

MR. PATTON: Can we go off the record?

(Off the record at 7:45 p.m.)

(Resume at 7:59 p.m.)

MR. TOOMEY: Could you please read back the last question?

(The reporter read back the question.)

MR. PATTON: Objection to the question to the extent it calls for classified information

and information subject to the statutory privileges.

To the extent the witness is aware of an unclassified answer, she may provide a response.

THE WITNESS: The only point I would provide to you on this, which is not necessarily anything new, but we still stand behind the information about how the filtering works in our Civil Liberties and Privacy Office Report, and that remains true today as it did in 2014, when we wrote the report.

BY MR. TOOMEY:

Q Is there classified information you're not providing in response to my question at the instruction of your lawyer?

A Yes.

Q Thank you. Similar question, apart from the unclassified information that you've already provided today, could you please describe in as much detail as necessary to give a complete answer how the change in April 2017 affected the

scanning of communications subject to upstream surveillance?

MR. PATTON: Object to the question, calls for classified information and information subject to statutory privileges, and instruct the witness not to answer the question.

THE WITNESS: I will not answer.

BY MR. TOOMEY:

Q Apart from the unclassified information you've already provided today, please describe in as much detail as necessary to give a complete answer which portions of an Internet transaction are scanned for selectors after April 2017?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q Since April 2017, does the NSA first scan the contents of communications for selectors, and then discard those that are solely about a

selector?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q Since April 2017, does the NSA copy the contents of communications prior to scanning those communications?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q Since April 2017, does the NSA copy the application layer data of packets prior to scanning the communications to which they belong?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the

instruction.

BY MR. TOOMEY:

Q Since April 2017, does the NSA review any portion of the contents of communications for selectors?

MR. PATTON: Object to the form, vague as to "review," and object to the question as seeking classified information, subject to the state secrets and statutory privileges, and instruct the witness not to answer.

THE WITNESS: Will follow the directions.

BY MR. TOOMEY:

Q Would your answer have been the same if I had said does the NSA scan any portion of the contents of communications for selectors --

MR. PATTON: One moment.

MR. TOOMEY: -- since April 2017?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: Could you rephrase the question in terms of an Internet transaction?

It's fine if you don't, but that might take care of something.

MR. TOOMEY: Sure, let me rephrase.

BY MR. TOOMEY:

Q Since April 2017, does the NSA scan any portion of the contents of Internet transactions for selectors?

(Counsel conferring.)

MR. PATTON: I think we need to go off the record.

MR. TOOMEY: Let's go off the record.

(Off the record at 8:04 p.m.)

(Resume at 8:18 p.m.)

MR. TOOMEY: Could you please read back the prior question?

(The reporter read back the question.)

MR. PATTON: Objection to the question to the extent it seeks classified information and information protected by the statutory privileges.

The witness can answer the question to the extent that it's unclassified.

THE WITNESS: So NSA scans a portion

of the Internet transaction to identify the task selector in order to acquire the Internet transaction that is to or from the target.

To go any further in terms of whether it's in the content or the metadata, or any of those further things, is classified.

MR. PATTON: And I instruct her not to answer beyond that unclassified answer.

BY MR. TOOMEY:

Q And you're following your counsel's instruction?

A I am.

Q So just to confirm, what portions of the contents of Internet transactions are scanned for selectors since April 2017?

MR. PATTON: I was waiting for you to finish.

Objection to the extent that it mischaracterizes the prior testimony. The witness can answer the question to the extent it's unclassified. Any classified answer, I instruct her not to provide.

THE WITNESS: You're asking me what portion of the Internet transaction we're scanning, just so I'm clarifying?

BY MR. TOOMEY:

Q Correct, after April 2017.

A After April 2017?

I am not able to answer that question. The answer to that question is classified.

Q Since April 2017, does the NSA review the entire contents of communication of Internet -- let me strike that. I'll restate the question.

Since April 2017, does the NSA scan the entire contents of Internet transactions for selectors?

MR. PATTON: Objection, calls for classified information, information protected by the statutory privileges, and instruct the witness not to answer.

THE WITNESS: I will follow the instructions.

BY MR. TOOMEY:

Q Since April 2017, does the NSA scan any portion of the application layer data of Internet transactions for selectors?

MR. PATTON: Same objection, same instructions.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q And if I were to ask what portions of Internet transaction the NSA scans for selectors, would your answer be the same?

MR. PATTON: Are we talking about post April 2017?

MR. TOOMEY: Yes, post April 2017.

MR. PATTON: Same objection, same instruction.

THE WITNESS: Yes, my answer would be the same.

BY MR. TOOMEY:

Q And since April 2017, does the NSA scan the entire application layer of Internet

transactions for selectors?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instructions.

BY MR. TOOMEY:

Q Are there any barriers to the NSA restarting "about" collection today?

MR. PATTON: Objection, beyond the scope of 30(b)(6) notice, calls for a legal conclusion.

THE WITNESS: NSA --

MR. PATTON: Just a second. There may be an additional objection.

(Counsel conferring.)

MR. PATTON: I would just add that to the extent that the question calls for a classified answer, I object to that based on the state secrets privilege and the statutory privileges. If there's an unclassified answer, the witness can provide.

And my colleague let's me know that

there's also a vagueness objection.

BY MR. TOOMEY:

Q You can answer to the extent --

A Sure. With the passage of the 702 FAA Reauthorization, there is a requirement for once the FISC has approved us going back to "abouts," that we have to give a 30-day notice to Congress before we can move forward with any type of collection.

MR. PATTON: Any type of "abouts" collection.

THE WITNESS: Any type of "abouts" collection. Apologies for not being clear.

BY MR. TOOMEY:

Q Do you consider that statutory requirement a barrier to the NSA restarting "about" collection?

MR. PATTON: Objection, beyond the scope of 30(b)(6), vague as to what a barrier is, calls for a legal conclusion.

The witness can answer in her own capacity.

THE WITNESS: Can you explain what you mean by barrier? I mean, to the extent -- yeah.

BY MR. TOOMEY:

Q I mean by barrier any obstacle, impediment to restarting "about" collection.

MR. PATTON: Same set of objections, and add in the one that to the extent there's any classified response to that, the witness should not answer as to classified information. You can otherwise provide an unclassified answer in your personal capacity.

THE WITNESS: Certainly getting FISC approval and notifying Congress are additional barriers beyond just being able to turn it on tomorrow.

BY MR. TOOMEY:

Q And could you please state whether there is any -- first of all, are there any other barriers besides the two that you just described?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: Go off the record.

(Off the record at 8:25 p.m.)

(Resume at 8:36 p.m.)

MR. TOOMEY: All right, let's go back on the record.

THE WITNESS: Can you read it back?

(The reporter read back the question.)

THE WITNESS: Are you answering first or am I?

MR. PATTON: Sorry, putting this away. Object to the question to the extent it calls for classified information and information protected by the statutory privileges. The witness can answer the question to the extent unclassified.

THE WITNESS: So as noted, the FISC would have to approve us going back to doing "abouts," so we would have to address any of the underlying issues as it relates to getting the FISC approval, as were described in the 2017 Memorandum Opinion.

BY MR. TOOMEY:

Q What are those underlying issues?

MR. PATTON: Object to the question to the extent it calls for classified information and information protected by the statutory privileges.

The witness can answer the question to the extent unclassified.

THE WITNESS: So the two unclassified descriptions that were provided in the 2017 Memorandum Opinion indicated there were both technological issues, as well as human error issues.

BY MR. TOOMEY:

Q And what were those issues?

MR. PATTON: Objection to the extent it calls for classified information and information protected by the statutory privileges.

The witness can answer to the extent unclassified.

THE WITNESS: Could I have the 2017 so I can point you to those sections? Do you want to introduce that in? Is that what's coming next?

MR. TOOMEY: Could you please mark that?

(Deposition Exhibit 51 was marked for identification.)

BY MR. TOOMEY:

Q Please take a look at Exhibit 51 which the court reporter has just handed you.

Could you tell me, are you familiar with this document and what it is?

A Yes. This is the Memorandum Opinion and Order of the Foreign Intelligence Surveillance Court dated April 26, 2017.

So I will start with page 14 to 15 --

MR. GILLIGAN: Sorry, did we mark this?

THE WITNESS: Yes, it's 51.

So the first indication of this discussion is starting at the bottom of page 14. The sentence begins, "The October 26, 2016 Notice disclosed that an NSA Inspector General review and report and NSA Office of Compliance for Operation verification activities indicated that, with greater frequency than previously disclosed to the Court, NSA analysts had used U.S.-person

identifiers to query the results of Internet 'upstream' collection, even though NSA's Section 702 minimization procedures prohibited such queries."

BY MR. TOOMEY:

Q So if I could stop you there.

A Sure.

Q Is it accurate to say that the technical and human error issues that the FISC identified related to queries of the results of Internet upstream collection?

(Counsel conferring.)

MR. PATTON: If the answer is yes or no, the witness can answer the question.

THE WITNESS: Yes.

BY MR. TOOMEY:

Q Besides the barriers you already identified and what's described in Exhibit 51, are there any other barriers to the NSA restarting "about" collection?

MR. PATTON: Objection to the extent that it calls for classified information and

information protected by the statutory privileges.

If there's an unclassified answer the witness can provide, she can provide it.

THE WITNESS: I'm sorry, can we go off the record?

(Off the record at 8:42 p.m.)

(Resume at 8:43 p.m.)

THE WITNESS: To the extent that NSA considers budget, time, intelligence needs, risk to the agency, privacy and civil liberties impact, all of those will also be considered as NSA decides whether or not to spend its next intelligence needs to go into "abouts."

Whether that's a particular barrier or not, those are all considerations that NSA will take into consideration as it thinks about whether or not it should go forward with "abouts."

BY MR. TOOMEY:

Q Okay. Is there any other barrier you haven't already described?

A No.

Q Has the NSA disavowed any intention of

resuming "about" collection in the future?

MR. PATTON: Just a second.

(Counsel conferring.)

MR. PATTON: Just object to beyond the scope of 30(b)(6). The witness can answer if she knows.

THE WITNESS: No.

BY MR. TOOMEY:

Q Has the NSA indicated to any member of Congress any interest in resuming "about" collection in the future?

MR. PATTON: Just a second.

(Counsel conferring.)

MR. PATTON: Same objection as beyond the scope of 30(b)(6). The witness can answer if she's aware.

THE WITNESS: Admiral Rogers testified that he would consider going back up on "abouts" collection if he could make it through all the -- you know, if it met the needs -- met intelligence needs, and they were in a position to meet all the needs of the FISC and notification to Congress.

BY MR. TOOMEY:

Q Do you know when Admiral Rogers provided that testimony?

A I want to say roughly October time frame 2018 -- I'm sorry, sorry 2017 -- in the future. Somewhere in the September/October 2017. It might have been part of one of the threat briefings.

Q Do you know to whom he provided that testimony? Which congressional committee or --

A I believe it was SSCI, Senate Select Committee on Intelligence. I'm pretty certain that's who it was.

Q Thank you.

A It could have been part of an appropriations hearing, but ...

Q And was that testimony public testimony?

A Yes, it was.

Q Has the NSA indicated to the FISC any interest in resuming "about" collection in the future?

MR. PATTON: Objection.

(Counsel conferring.)

MR. PATTON: The objection is twofold. One, beyond the scope of 30(b)(6) and, two, object to the extent it calls for a classified answer, and also one subject to statutory privileges. But if the witness is personally aware of that fact and it's unclassified, she can answer.

THE WITNESS: The answer is classified, and I'm following the instructions of my lawyer.

BY MR. TOOMEY:

Q Has the NSA indicated to the FISC that it intends to resume "about" collection in the future?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Same answer.

MR. TOOMEY: Can we mark as the next exhibit, please, this document?

(Deposition Exhibit 52 was marked for identification.)

BY MR. TOOMEY:

Q Could you please take a look at Exhibit 52 and tell me if you recognize this document and what it is?

A I recognize this document. It is the NSA press release dated April 28, 2017, stating, "NSA Stops Certain Foreign Intelligence Collection Activities Under Section 702."

Q Thank you. Let me move to a different -- can we please mark this document as Exhibit 53?

(Deposition Exhibit 53 was marked for identification.)

BY MR. TOOMEY:

Q Could you please take a look at this document, state whether you're familiar with it, and describe it.

A Yes, I am familiar with it. It is the statement from April 28th, 2017, stating, "NSA Stops Certain Section 702 'Upstream' Activities."

Q And I'm going to read a short passage from the first paragraph at the end, which says,

"After a comprehensive review of mission needs, current technological constraints, United States person privacy interests, and certain difficulties in implementation, NSA has decided to stop some of its activities conducted under Section 702."

Is that sentence accurate?

A Yes.

Q Did any court order the NSA to stop "about" collection?

MR. PATTON: One second.

(Counsel conferring.)

MR. PATTON: My only objection is to vagueness as to the term "stop" in the context of a court order.

MR. GILLIGAN: Beyond the scope.

MR. PATTON: It's also beyond the scope then.

MR. TOOMEY: You can answer.

THE WITNESS: Actually, I would just like more specificity. What are you -- I'm not sure I entirely understand.

If you read -- maybe I'll give a

little bit more answer. If you read on the second page of Exhibit 53, it states, "After considerable evaluation of the program and available technology, NSA has decided that its Section 702 foreign intelligence surveillance activities will no longer include any upstream internet communications that are solely 'about' a foreign intelligence target."

So could you be clearer of the particular court?

BY MR. TOOMEY:

Q Could you read me the title of Exhibit 53?

A Sure. NSA statement, "NSA Stops Certain Section 702 'Upstream' Activities," dated April 28th, 2017.

Q And my question is did any court order the NSA to stop "about" collection?

MR. PATTON: Same objections.

THE WITNESS: Can you describe what court you're talking about?

BY MR. TOOMEY:

Q I'm asking about any court.

A Any court?

Q But any court would include the FISC.

MR. PATTON: Same objections. Also, this particular one calls for a legal conclusion too. You can answer.

THE WITNESS: Okay.

So the Attorney General and the DNI put forward a set of targeting procedures to the FISC, and the FISC agreed with those procedures. There was no FISC ordering us to stop.

BY MR. TOOMEY:

Q Did Congress prohibit the NSA from conducting "about" collection in April of 2017?

MR. PATTON: Objection, vague as to April 2017. Same set of objections as before, beyond the scope of 30(b)(6), calls for a legal conclusion, vague.

THE WITNESS: No.

BY MR. TOOMEY:

Q Congress hasn't since prohibited the

NSA from restarting "about" collection, correct?

MR. PATTON: Objection, beyond the scope, calls for a legal conclusion.

THE WITNESS: With the passage of the 702 FAA Reauthorization, it puts in place a requirement for notification 30 days between when the FISC approves it and when we could start, unless there's extenuating circumstances.

BY MR. TOOMEY:

Q So that statute doesn't contain a prohibition on restarting "about" collection?

A Correct.

MR. PATTON: Same set of objections.

THE WITNESS: Correct.

BY MR. TOOMEY:

Q Today, does upstream surveillance involve the scanning of all international text-based communications on individual circuit or circuits the NSA is monitoring?

MR. PATTON: Objection, calls for classified information and information protected by the statutory privileges.

Instruct the witness not to answer.

THE WITNESS: I will follow instructions.

MR. GILLIGAN: Could I hear the question again, please?

(The reporter read back the question.)

MR. GILLIGAN: Can we go talk, please? Off the record.

(Off the record at 8:57 p.m.)

(Resume at 9:22 p.m.)

BY MR. TOOMEY:

Q Let's go back on the record.

Ms. Jaques, could you please read back the last question?

(The reporter read back the question.)

MR. PATTON: Objection to the question, that calls for a classified answer, and also an answer that seeks information protected by the statutory provisions.

Instruct the witness not to answer.

THE WITNESS: I will follow the instructions.

MR. TOOMEY: So going forward, can we shorten that to assert state secrets and statutory privileges?

MR. PATTON: I will shorten it as fast as I can.

BY MR. TOOMEY:

Q In June 2015, did upstream surveillance involve the scanning of all international text-based communications on the individual circuit or circuits the NSA was monitoring?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instructions.

BY MR. TOOMEY:

Q Today, if some international text-based communications on a given circuit are not scanned, please explain in as much detail as necessary to completely answer why those communications are not scanned.

MR. PATTON: Please repeat the

question.

(The reporter read back the question.)

MR. PATTON: Object to the question to the extent it calls for classified information and information protected by the statutory privileges.

The witness can answer the question to the extent that she is aware of an unclassified answer to that question.

THE WITNESS: Can you read the question one more time to make sure I have it entirely accurate?

(The reporter read back the question.)

THE WITNESS: As we were discussing in the existing Civil Liberties and Privacy Report, the process is that there's filtering, and then there's scanning. So to the extent that we have filtered wholly domestic communications out as part of that, those would not be scanned.

BY MR. TOOMEY:

Q Beyond that response and beyond the unclassified information you've already provided today, can you please fully explain in as much

detail as necessary why some communications are not scanned?

MR. PATTON: Object to the question, calls for classified information, information protected by the statutory privileges.

Instruct not to answer.

THE WITNESS: Will follow the instructions.

BY MR. TOOMEY:

Q Same question as of June 2015. If you need me to restate the question, I can.

A Can you restate the question?

Q Apart from the unclassified information you've already provided today, as of June 2015, if some international text-based communications on a given circuit were not scanned, please explain in as much detail as necessary to fully answer why those communications are not scanned.

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: Object to the question,

calls for classified information and information protected by the statutory privileges.

If there's any information that the witness is aware of that has not already been provided either in the interrogatory responses or in the prior testimony that would answer that question, she can go ahead and give it.

If not, I would instruct her not to answer the question based on those privileges.

THE WITNESS: There's no additional information, so I'll follow counsel's directions.

BY MR. TOOMEY:

Q There's no additional unclassified information?

A There's no additional unclassified information that I can provide you beyond what we've already provided you.

Q And there is classified information which you're not providing based on your counsel's instruction?

MR. PATTON: To the extent that the answer to that question is yes or no, you can

answer the question.

THE WITNESS: Yes, that's correct.

MR. TOOMEY: Thank you. Let's go off record.

(Off the record at 9:29 p.m.)

(Resume at 9:39 p.m.)

EXAMINATION BY COUNSEL FOR PLAINTIFFS

BY MS. HANLEY COOK:

Q Hi, I'm Devon Hanley Cook. We spent the day together, but nice to meet you. I want to thank you for your patience and for putting up with all our questions and going so late today. I also want to thank you, Dawn. I know it's been a really long day for everybody.

Does NSA now scan Wikimedia's communications in the course of upstream surveillance?

MR. PATTON: Objection, calls for classified information, subject to state secrets privilege and to statutory privileges.

Instruct the witness not to answer.

THE WITNESS: I will follow the

instructions.

BY MS. HANLEY COOK:

Q In 2015, did NSA scan Wikimedia communications in the course of upstream surveillance?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MS. HANLEY COOK:

Q Does NSA now copy Wikimedia communications in the course of upstream surveillance?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MS. HANLEY COOK:

Q In June 2015, did NSA copy Wikimedia communications in the course of upstream surveillance?

MR. PATTON: Same objection, same

instruction.

THE WITNESS: Will follow the instruction.

BY MS. HANLEY COOK:

Q Has NSA acquired Wikimedia communications as a result of upstream surveillance now?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MS. HANLEY COOK:

Q As of June 2015, had NSA acquired Wikimedia communications as a result of upstream surveillance?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instructions.

BY MS. HANLEY COOK:

Q Can I have Tab X, please? Let's save time, let's do X and Y, please.

MR. GILLIGAN: 54 and 55 then?
THE REPORTER: Yes, 54 and 55.
(Deposition Exhibits 54 and 55 were marked for identification.)
BY MS. HANLEY COOK:
Q Let's start with Exhibit 54.
Have you seen Exhibit 54 before?
MR. PATTON: Just a second.
(Counsel conferring.)
MR. PATTON: Object to the question as beyond 30(b)(6). The witness can answer yes or no if she has personally seen this Exhibit 54 before.
THE WITNESS: No.
BY MS. HANLEY COOK:
Q If you assumed that Exhibit 54 related to upstream surveillance, it would indicate, wouldn't it, that the NSA had an intelligence interest in Wikimedia's communications, wouldn't it?
MR. PATTON: Object to the question, calls for a classified answer, subject to the state secrets privilege and to the statutory

privileges.

Instruct the witness not to answer the question.

THE WITNESS: Will follow those instructions.

BY MS. HANLEY COOK:

Q Turning to Exhibit 55, have you seen this document before? Actually, let me -- Exhibit 54. Recognizing that you have not seen the document before, what do you think it is?

MR. PATTON: Objection. Same objection as before, same instruction.

THE WITNESS: Which instruction was that? Classified?

MR. PATTON: Classified, subject to the state secrets privilege and to statutory privileges.

The witness is instructed not to answer the question.

THE WITNESS: I will follow those instructions. I just had to make sure I knew what the instructions were.

BY MS. HANLEY COOK:

Q Makes sense.

Exhibit 55, have you seen this document before?

MR. PATTON: Object to the question to the extent it's beyond 30(b)(6). The witness can answer yes or no if she has seen this document in her personal capacity.

THE WITNESS: Yes.

BY MS. HANLEY COOK:

Q What is it?

MR. PATTON: Object to the question, calls for a classified answer, subject to the state secrets and to statutory privileges.

Instruct the witness not to answer.

THE WITNESS: I will follow those instructions.

BY MS. HANLEY COOK:

Q If you assumed that Exhibit 55 related to upstream surveillance, it would indicate, wouldn't it, particularly on the second page in the first bullet point, that the NSA has an

intelligence interest in Wikimedia's HTTP communications, wouldn't it?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow those instructions.

BY MS. HANLEY COOK:

Q Do Exhibits 54 or 55 relate to upstream surveillance?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow those instructions.

BY MS. HANLEY COOK:

Q At this time, HTTP communications are scanned for selectors in the course of upstream surveillance, aren't they?

MR. PATTON: Just a second.

(Counsel conferring.)

MR. PATTON: Same objection, same instructions. Do you need a reminder on the --

THE WITNESS: I just need to remind

what --

MR. PATTON: Do you need the question read back?

THE WITNESS: Could you read the question again?

(The reporter read back the question.)

MR. PATTON: Object to the question, calls for classified information, information protected by the statutory privileges, and instruct the witness not to answer.

THE WITNESS: I will follow those instructions.

BY MS. HANLEY COOK:

Q As of June 2015, HTTP communications were scanned for selectors in the course of upstream surveillance, right?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instructions.

BY MS. HANLEY COOK:

Q At this time, HTTPS communications are

scanned for selectors in the course of upstream surveillance, aren't they?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MS. HANLEY COOK:

Q Same question as to the June 2015 time frame.

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MS. HANLEY COOK:

Q Are Apache Kafka communications scanned for selectors in the course of upstream surveillance?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MS. HANLEY COOK:

Q Do you know what Apache Kafka communications are?

MR. PATTON: Object to the question, beyond the scope, calls for expert testimony.

The witness can answer in her personal capacity.

THE WITNESS: Not well enough to describe to you.

BY MS. HANLEY COOK:

Q Open VPN communications are scanned for selectors in the course of upstream surveillance, aren't they?

MR. PATTON: Objection, vague as to time period, calls for classified information and information protected by the statutory privileges.

Instruct the witness not to answer.

THE WITNESS: Will follow the instruction.

BY MS. HANLEY COOK:

Q As of June 2015, were open VPN communications scanned for selectors in the course

of upstream surveillance?

MR. PATTON: Same objection without the vague as to time.

Same instruction not to answer.

THE WITNESS: Will follow the instruction.

BY MS. HANLEY COOK:

Q Other than public documents, public documents at large, hearing testimony that is transcribed, public documents you reviewed, documents that have been filed or served in this case, or your testimony today, what can you tell me about the volume of communications subject to upstream surveillance at this time using any unit of measurement you want to discuss volume of communications?

MR. PATTON: Just one moment.

Can we go off the record?

(Off the record at the 9:49 p.m.)

(Resume at 9:49 p.m.)

MR. PATTON: Could you read back the question, please?

(The reporter read back the question.)

MR. PATTON: Other than the officially disclosed government statements, whether they be publicly by ODNI or by NSA or filed in this particular case or filed in the FISC and declassified, any other information that the witness would have would be classified, and so I would instruct her not to answer the question based on the state secrets privilege and statutory privileges.

THE WITNESS: I'll follow the instructions.

BY MS. HANLEY COOK:

Q Okay. How many communications -- and you can use any unit of measurement you want -- did NSA retain as a result of upstream surveillance in each of the last three years?

MR. PATTON: Objection, vague as to the term "communication," and classified, subject to the state secrets privilege and statutory privileges, and instruct not to answer.

THE WITNESS: Will follow the

instruction.

BY MS. HANLEY COOK:

Q Same question as to transactions.

MR. PATTON: Same objections except for vagueness, same instruction.

THE WITNESS: I will follow the instructions.

BY MS. HANLEY COOK:

Q What is the volume of communications copied in the course of upstream surveillance in each of the last three years?

MR. PATTON: Objection, vague. Objection, seeks classified information protected by the state secrets privilege, statutory privileges, instruct not to answer.

THE WITNESS: I will follow the instructions.

BY MS. HANLEY COOK:

Q Same question as to transactions.

MR. PATTON: Same objections with exception of vagueness, same instruction.

THE WITNESS: Following the

instructions.

BY MS. HANLEY COOK:

Q What is the volume of communications or transactions that are subject to filtering in the course of upstream surveillance in the last three years?

MR. PATTON: I'm sorry, did you use the term "Internet transactions"?

MS. HANLEY COOK: No.

MR. PATTON: I'm sorry, could you read the question back?

(The reporter read back the question.)

MR. PATTON: Objection, vague as to communications, and objection to the rest for the same reasons set forth before, instruct not to answer.

THE WITNESS: Will follow the instructions.

BY MS. HANLEY COOK:

Q Would the answer be the same if I used the term "Internet transactions"?

MR. PATTON: The instruction not to

answer would be the same, but there would be no vagueness objection, if that helps, or deemed compound since it was previous communications or transactions, but the instruction not to answer would remain the same, yes.

(Deposition Exhibit 56 was marked for identification.)

BY MS. HANLEY COOK:

Q Please take a look at Exhibit 56. Have you seen this document before?

MR. PATTON: We need to go off the record.

MS. HANLEY COOK: Okay.

(Off the record at 9:53 p.m.)

(Resume at 9:59 p.m.)

BY MS. HANLEY COOK:

Q The question was have you seen this document before?

MR. PATTON: Objection as beyond the scope of 30(b)(6). The witness can answer in her personal capacity if she's seen the document before.

THE WITNESS: I've certainly seen portions of it. I'm not sure I saw it in its entirety when I was working at DHS. I don't know that I saw it all in its entirety.

BY MS. HANLEY COOK:

Q What is it?

MR. PATTON: Same objection.

THE WITNESS: Memorandum Opinion for the Counsel to the President on legal issues relating to the testing, use, and deployment of an intrusion detection system (Einstein 2.0) to protect unclassified computer networks in the Executive Branch, dated January 9, 2009.

BY MS. HANLEY COOK:

Q Thank you. Please turn to page 4 of Exhibit 56, the second paragraph that begins "EINSTEIN 2.0."

A Mm-hmm.

Q I'd like you to read the first two sentences to yourself, and tell me when you're done.

A (Witness reviewing document.) Yeah.

Q Exhibit 56 says that Einstein 2.0 sensors will scan a temporary copy of traffic, right?

MR. PATTON: Same objections.

THE WITNESS: That's what the sentence says, yes.

BY MS. HANLEY COOK:

Q Is that sentence containing "temporary copy" accurate to the best of your knowledge?

MR. PATTON: Same objection, lack of foundation as well.

THE WITNESS: To the extent that I at some point reviewed a Privacy Impact Assessment associated with Einstein 1 or Einstein 2, it was many years ago, so I can't speak to whether the specificity -- I didn't review this document in advance of any of this conversation, so I would want to go back and look at all those materials before I gave you an answer one way or the other.

I have no reason to say it's not, but I have no reason to know whether that was exactly how it was implemented, or whether it remains true

today.

BY MS. HANLEY COOK:

Q But this document at least says that it will create a temporary copy, right?

MR. PATTON: Objection, the document speaks for itself.

THE WITNESS: Yes, that's what the sentence says.

BY MS. HANLEY COOK:

Q The next sentence that I had you read says that, "Einstein 2.0 operations will not disrupt the normal operations of federal systems."

Did I read that right?

A Yes, you did.

Q Do you know why Einstein 2 involves the creation of a temporary copy of the traffic being scanned?

MR. PATTON: Objection, beyond the scope of 30(b)(6), calls for -- it also -- it also indicates I'm getting tired -- beyond the scope and lacks foundation.

THE WITNESS: Well, you can read the

words that are on the page.

BY MS. HANLEY COOK:

Q Do the words on this page indicate to you why Einstein 2 involves the creation of a temporary copy of the traffic being scanned?

MR. PATTON: Same objections.

THE WITNESS: Well, it says it's for the purpose of scanning by the sensors. I guess that's not the why.

BY MS. HANLEY COOK:

Q Doesn't Einstein 2 create a temporary copy of the traffic being scanned so that it will not disrupt the normal operations of federal systems?

MR. PATTON: Same objections, including lack of foundation.

THE WITNESS: I'm not -- again, in my personal capacity, having done work on this in previous positions, without having reviewed all those documents, I'm not willing to expound one way or the other on the particular information provided here beyond what you see on the piece of

paper.

BY MS. HANLEY COOK:

Q In June 2015, did upstream surveillance involve the scanning of a temporary copy of the transactions scanned?

MR. PATTON: Objection, calls for classified information, information subject to the statutory privileges, and instruct the witness not to answer.

THE WITNESS: I will follow the instructions.

BY MS. HANLEY COOK:

Q Going back several hours now --

A Awesome.

Q -- you testified I think, but correct me if I'm wrong, that as of June 2015, the NSA scanned at least some portions of the application layer of Internet transactions as part of upstream collection, right?

MR. PATTON: Just a second.

(Counsel conferring.)

MR. PADGETT: Can you read the

question?

(The reporter read back the question.)

THE WITNESS: Can we go off the record?

MS. HANLEY COOK: Yeah, thank you.

(Off the record at 10:06 p.m.)

(Resume at 10:11 p.m.)

THE WITNESS: Can you repeat your sentence one more time to make sure I was accurately -- or can you repeat what you --

MS. HANLEY COOK: Dawn, do you mind reading it? Thanks.

(The reporter read back the question.)

THE WITNESS: Yes, that's correct.

BY MS. HANLEY COOK:

Q You also testified that deep packet inspection refers to the scanning of the application layer of Internet packets, right?

A In the general -- oh.

MR. PATTON: Object to the extent it may mischaracterize the testimony, and beyond the scope, but the witness can answer.

THE WITNESS: In the general sense, as is traditionally understood for what deep packet inspection means, not specific to upstream.

BY MS. HANLEY COOK:

Q But it's accurate then to say that upstream surveillance, as of June 2015, involved deep packet inspection, right?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: Objection as to vague, beyond the scope of 30(b)(6), and to the extent there's any classified information, instruct the witness not to answer.

If there's an unclassified answer that she can provide, she can provide that now.

THE WITNESS: I have no further information. I will take the instructions and not provide classified information.

BY MS. HANLEY COOK:

Q Today, how many targets does NSA have for upstream surveillance?

MR. PATTON: Objection, calls for

classified information, and information protected by the statutory privileges, instruct not to answer.

THE WITNESS: Could you ask the question again, please?

BY MS. HANLEY COOK:

Q Sure. Today how many targets does NSA have for upstream surveillance?

MR. PATTON: Same objection. If the witness is aware of any unclassified answer, we should probably talk about that.

THE WITNESS: Okay, why don't we go talk about that.

MR. PATTON: Off the record.

(Off the record at 10:14 p.m.)

(Resume at 10:14 p.m.)

MR. PATTON: Read the question back, please.

(The reporter read back the question.)

MR. PATTON: Same objections, same instructions.

THE WITNESS: I will follow the

instructions.

BY MS. HANLEY COOK:

Q In June 2015, how many targets did NSA have for upstream surveillance?

MR. PATTON: Same objection, same instruction.

THE WITNESS: I'll follow the instructions.

BY MS. HANLEY COOK:

Q Without revealing the -- you good?

MR. PATTON: Yeah.

BY MS. HANLEY COOK:

Q Without revealing the contents of any conversations that you had with your attorneys outside this room today, and with the exception of conversations related to determining whether classified information was responsive to a question, where the line was properly drawn on classified information, state secret classifications, during breaks in the deposition today, did you discuss with anyone the substance of your testimony during the deposition?

MR. PATTON: Subject to those caveats you said, plus the statutory privileges, the witness can answer.

THE WITNESS: No.

MS. HANLEY COOK: I have no further questions.

MR. TOOMEY: Can we take a break?

MS. HANLEY COOK: Strike that I said that. Take a break for five minutes to be sure, just go back through the outline.

(Off the record at 10:16 p.m.)

(Resume at 10:26 p.m.)

FURTHER EXAMINATION

BY MR. TOOMEY:

Q When a communication is encrypted using HTTPS, does some of the communication's metadata remain unencrypted?

MR. PATTON: One second.

(Counsel conferring.)

MR. PATTON: Object to the question as beyond the scope of 30(b)(6), calling for an expert opinion. The witness can answer in her

personal capacity to the extent that she is aware of the answer.

THE WITNESS: In the general sense, it will depend on the type of encryption that's being used, and it will depend on the nature of how it's being transmitted, so there's not one answer that fits all.

BY MR. TOOMEY:

Q So when a communication is encrypted using HTTPS, does some of the communication's metadata remain unencrypted?

MR. PATTON: Object to the term "communication" as vague, and same prior objections and instruction to the witness.

THE WITNESS: To the extent that the question is somewhat vague, I'll say generally speaking, yes, but I think there are different ways you could do things that might change that answer.

BY MR. TOOMEY:

Q When a communication is encrypted using HTTPS, are the senders and recipients'

IP addresses unencrypted?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Generally speaking, they will -- I'm sorry, say the question one more time.

(The reporter read back the question.)

MR. PATTON: Same objection, same instruction.

THE WITNESS: Again, the question is somewhat vague, and so I would answer generally that is true, but there are undoubtedly a number of exceptions that also could make that untrue.

MR. TOOMEY: Could you please mark this document as 57.

(Deposition Exhibit 57 was marked for identification.)

BY MR. TOOMEY:

Q Could you please take a look at the document, describe what it is, and tell me if you're familiar with it.

A This is the Notice of Filing of Government's Responses to FISC Questions Regarding

the Amended 2011 Section 702 Certifications, dated November 15th, 2011.

Q Thank you.

A Yes, I am familiar with these documents.

Q Could you please turn to page 9?

A Sure.

Q I'm going to read from about the third paragraph down in the middle of the personal knowledge, which says, "Metadata that has been extracted from Internet transactions consistent with Section 3(b)(5)(b)(4) is subject to the two-year retention limit set forth in Section 3(c) of the amended NSA minimization procedures."

Was that statement accurate at the time this document was filed with the FISC on November 15th, 2011?

A Yes.

Q So the NSA extracts metadata from communications collected in the course of upstream surveillance, correct?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: Objection, vague as to time period, but the witness can answer.

THE WITNESS: Could you ask the question again?

(The reporter read back the question.)

MR. PATTON: Objection, vague as to time.

THE WITNESS: So I would just offer that the answer to your question is metadata has been extracted from the Internet transactions. I believe that the question said communications, in which case that would be consistent with the information that was provided here.

BY MR. TOOMEY:

Q So I'll rephrase.

The NSA extracts metadata from Internet transactions collected in the course of upstream surveillance, correct?

MR. PATTON: Objection, vague as to time.

THE WITNESS: Consistent with 2011,

what's written here at 2011, yes, that is true.

BY MR. TOOMEY:

Q Today, the NSA retains metadata associated with its targets' communications in the course of upstream surveillance, correct?

MR. PATTON: Hold on.

(Counsel conferring.)

MR. PATTON: Sorry, could you read the question back, please?

(The reporter read back the question.)

MR. PATTON: Object to the question to the extent it calls for classified information or otherwise privileged pursuant to the aforementioned statutes.

If there is an unclassified answer, the witness can provide it.

THE WITNESS: Could you read the question one more time?

(The reporter read back the question.)

MR. PATTON: Same objection, same instruction.

THE WITNESS: NSA retains -- I would

again go back to, instead of saying "communications," I would say "Internet transaction." I would say generally, yes, this is true.

BY MR. TOOMEY:

Q Sorry, I didn't hear you. Could you say that again?

A Sure. NSA retains metadata -- may retain metadata associated with Internet transactions in the course of upstream.

Q The NSA has an interest in the metadata of its targets' communications or Internet transactions, correct?

MR. PATTON: Objection as vague, beyond the scope of 30(b)(6).

The witness can answer.

THE WITNESS: NSA is interested in the metadata associated with the Internet transactions of a targeted selector -- to or from a targeted selector.

BY MR. TOOMEY:

Q So just to be clear, just to make sure

I understood your answer, the NSA has an interest in the metadata of communications to and from a targeted selector?

MR. PATTON: Objection, beyond the scope. The witness can answer.

THE WITNESS: Could you repeat the question?

(The reporter read back the question.)

THE WITNESS: I would not use the word "communications." I would use the word "Internet transactions."

BY MR. TOOMEY:

Q So just to be clear, the NSA has an interest in the metadata of Internet transactions to and from a targeted selector?

MR. PATTON: Objection, beyond the scope, asked and answered.

THE WITNESS: Yes.

MR. TOOMEY: Thank you. All right, we do not have any further questions right now.

MR. PATTON: Before we get off the record, the government is going to invoke Federal

Rule of Civil Procedure 30(e) to reserve the right to review and signature of the witness.

(Whereupon, at 10:36 p.m., the taking of the deposition was concluded. Reading and signature were reserved.)

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION,	:	
Plaintiff,	:	Case No.
vs.	:	
NATIONAL SECURITY AGENCY, et al.,	:	1:15-cv-00662-TSE
Defendants.	:	

ACKNOWLEDGMENT OF DEPONENT

I, REBECCA J. RICHARDS, do hereby acknowledge that I have read and examined pages ~~11~~ 9 through ~~239~~ 359 of the transcript of my deposition taken on Monday, April 16, 2018, and that:

(Check appropriate box):

( ) the same is a true, correct and complete transcription of the answers given by me to the questions therein recorded.

(X) except for the changes noted in the attached errata sheet, the same is a true, correct and complete transcription of the answers given by me to the questions therein recorded.

5/15/18
DATE

SIGNATURE

Wikimedia Foundation v. NSA, et al., 15-cv-00662-TSE (D. Md.)

ERRATA SHEET of REBECCA J. RICHARDS

Page	Line	To	From	Justification
9	8	Kathleen	Cathleen	Spelling Error
45	4	Michael S. Rogers	Michael F. Rogers	Spelling Error
161	19	telecom	teleco	Spelling Error
169	19	USA FREEDOM Act	USA Freedom Act	Capitalization
192	6	Protocol	protocol	Capitalization
196	13	(with our targeting procedures)	in parens	Transcription Error
263	17	scanned	scan	Clarification

CERTIFICATE OF NOTARY PUBLIC

I, DAWN A. JAQUES, a Notary Public in and for the District of Columbia, before whom the foregoing deposition was taken, do hereby certify that witness whose testimony appears in the foregoing pages was duly sworn by me; that the testimony of said witness was taken by me in shorthand at the time and place mentioned in the caption hereof and thereafter reduced to typewriting under my supervision; that said deposition is a true record of the testimony given by said witness; that I am neither counsel for, related to, nor employed by any of the parties to the action in which this deposition is taken; and, further, that I am not a relative or employee of any attorney or counsel employed by the parties thereto, nor financially or otherwise interested in the outcome of the actions.

Dawn A. Jaques

Dawn A. Jaques, CSR, CLR
Notary Public in and for
District of Columbia

My commission expires:
January 14, 2020

*** ERRATA SHEET ***
TRANSPERFECT DEPOSITION SERVICES
216 E. 45th Street, Suite #903
NEW YORK, NEW YORK 10017
(212) 400-8845

CASE: WIKIMEDIA FOUNDATION v. NATIONAL SECURITY AGENCY, et al.
DATE: APRIL 16, 2018
WITNESS: REBECCA J. RICHARDS REF: 21368

PAGE	LINE	FROM	TO

_____
REBECCA J. RICHARDS

Subscribed and sworn to before me

this ____ day of _____, 20__.

_____
Notary Public

B

C

N

O

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION,	)	
Plaintiff,	)	
	)	
v.	)	**Case No. 1:15-cv-662**
	)	
NATIONAL SECURITY AGENCY/ CENTRAL SECURITY SERVICE, *et al.*,	)	
	)	
Defendants.	)	

MEMORANDUM OPINION

At issue in this First and Fourth Amendment suit is plaintiff's motion to compel defendants to respond to discovery requests regarding defendant National Security Agency's ("NSA") Upstream surveillance program. Specifically, plaintiff served 84 discovery requests on defendants in an effort to establish that at least one of plaintiff's communications has been intercepted, copied, and reviewed by defendants. Defendants have objected to 53 of these requests on the basis of the common law state secrets privilege and other statutory privileges, arguing that the information plaintiff seeks, if disclosed, reasonably could be expected to result in exceptionally grave damage to U.S. national security. Plaintiff now moves for an order compelling defendants to produce any information responsive to plaintiff's requests, contending that the Foreign Intelligence Surveillance Act ("FISA")[1] displaces the common law state secrets privilege and establishes procedures for the *ex parte* and *in camera* review of sensitive national security information. These issues have been fully briefed and argued and are now ripe for disposition.

[1] 50 U.S.C. § 1801, *et seq.*

I.

A brief summary of the statutory framework pertinent to defendants' electronic surveillance efforts provides context necessary for resolution of the question presented in this case. In 1978, Congress enacted FISA in response to growing concerns about the Executive Branch's use of electronic surveillance. Specifically, Congress sought through FISA to accommodate U.S. national security interests in obtaining intelligence about foreign powers while also providing meaningful checks on the Executive Branch's ability to conduct that surveillance. In this respect, FISA created a "secure framework by which the Executive Branch may conduct legitimate electronic surveillance for foreign intelligence purposes within the context of this Nation's commitment to privacy and individual rights." S. Rep. No. 604, pt. 1, 95th Cong. 1st Sess. 15 (1977), reprinted in U.S.Code Cong. & Admin.News 1978, pp. 3904, 3916.

A central component of this framework is the U.S. Foreign Intelligence Surveillance Court ("FISC"). FISC, a tribunal composed of eleven federal district judges designated by the Chief Justice of the U.S. Supreme Court, is charged with the review of applications for electronic surveillance. *See* 50 U.S.C. § 1803(a). FISA provides that, with limited exceptions, the Executive Branch cannot conduct surveillance of a foreign power or its agents absent prior FISC authorization. To obtain FISC authorization for electronic surveillance, the Attorney General must personally approve an application for surveillance, which must (i) comport with FISA's procedural requirements and (ii) establish probable cause to believe that the target of electronic surveillance is a foreign power or an agent of a foreign power and that each of the facilities at which electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power. *Id.* § 1805

FISA also establishes rules governing the use of information obtained through electronic surveillance. *See id.* § 1806. Specifically, if the Government, including any State or political subdivision, intends to "enter into evidence or otherwise use or disclose" at any proceeding information obtained through electronic surveillance against an "aggrieved person"—that is, any person who has been the subject of electronic surveillance—the Government must first "notify the aggrieved person and the court or other authority" of its intent to so disclose or use the information. *Id.* §§ 1806(c),(d). The person against whom the evidence is to be introduced may then move to suppress the evidence obtained through electronic surveillance on the grounds that (i) "the information was unlawfully acquired" or (ii) "the surveillance was not made in conformity with an order of authorization or approval." *Id.* § 1806(e). FISA establishes specific procedures that courts must follow in the event (i) that the government notices its intent to use electronic surveillance information, (ii) that an aggrieved person files a motion to suppress or (iii) that an aggrieved person files "any motion . . . pursuant to any other statute or rule of the United States . . . to discover, obtain, or suppress" information obtained from electronic surveillance. *Id.* § 1806(f). Specifically, the court

> shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure . . . would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary . . . ."

Id.

On the basis of its *ex parte* and *in camera* review of the materials at issue, the court must determine "whether the surveillance of the aggrieved person was lawfully authorized and conducted." *Id.* FISA permits courts making this determination to disclose to the aggrieved person portions of the application, order, or other materials "only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." *Id.* If, in the end, the court

determines that the surveillance was not lawfully authorized or conducted, the court must suppress the unlawfully obtained evidence or otherwise grant the motion of the aggrieved person. *Id.* § 1806(g). If, on the other hand, the surveillance was lawfully authorized and conducted, the court "shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure." *Id.*

In addition to mandating specific procedures governing the use of information obtained through electronic surveillance, FISA establishes additional checks on the Executive's use of electronic surveillance. Two such checks come by way of criminal sanctions and a civil cause of action. Specifically, FISA imposes criminal penalties on any person who intentionally "engages in electronic surveillance under color of law except as authorized by [FISA]" or "discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by [FISA.]" *Id.* § 1809(a)(1)-(2). FISA also provides a civil cause of action to any "aggrieved person . . . who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 1809 . . . against any person who committed such violation . . . ." *Id.* § 1810.

In 2008, thirty years after FISA's enactment, Congress passed the FISA Amendments Act ("FAA"), which establishes additional procedures and requirements for the authorization of surveillance targeting persons located outside the United States. *See* 50 U.S.C. § 1881a-g. Specifically, § 702 of the FAA[2] provides that the Attorney General and the Director of National Intelligence may jointly authorize, for up to one year, the "targeting of [non-U.S.] persons reasonably believed to be located outside the United States to acquire foreign intelligence

[2] 50 U.S.C. § 1881a.

information" if the FISC approves "a written certification" submitted by the government attesting, *inter alia*, (i) that a significant purpose of the acquisition is to obtain foreign intelligence information and (ii) that the acquisition will be conducted "in a manner consistent with the [F]ourth [A]mendment" and the targeting and minimization procedures required by statute. 50 U.S.C. § 1881a(b),(g). To approve such a certification, the FISC must determine that the government's targeting procedures are reasonably designed:

> (i) to ensure that acquisition "is limited to targeting persons reasonably believed to be located outside the United States," *id.* § 1881 a(i)(2)(B)(i);
>
> (ii) to prevent the intentional acquisition of wholly domestic communications, *id.* § 1881a(i)(2)(B)(ii);
>
> (iii) to "minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign-intelligence information," *id.* § 1801(h)(1); *see id.* § 1881a(i)(2)(C); and
>
> (iv) to ensure that the procedures "are consistent with . . . the [F]ourth [A]mendment," *id.* § 1881a(i)(3)(A).

Unlike FISA, these FAA procedures do not require the FISC to determine that probable cause exists to believe that the target of electronic surveillance is a foreign power and that each of the facilities at which electronic surveillance is directed is being used or is about to be used by a foreign power.

The recent release of public reports and declassification of FISC opinions have revealed additional details regarding the collection of communications under § 702. For example, the government has disclosed that it conducts § 702 surveillance through two programs—PRISM and Upstream surveillance. *See* Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* 7 (2014) ("PCLOB Report"). The program at issue here, Upstream surveillance, involves

collection of communications of persons reasonably believed to be outside of the United States "with the compelled assistance . . . of the providers that control the telecommunications backbone over which [telephone and Internet] communications transit." *Id.* at 35. In this respect, "[t]he government 'tasks' certain 'selectors,' such as telephone numbers or email addresses, that are associated with targeted persons, and it sends these selectors to electronic communications service providers to begin acquisition." *Id.* at 7. The providers then assist the government in the collection of the communications associated with those selectors. *See id.*

II.

With this statutory framework in mind, it is appropriate to turn to the facts and procedural history in this case. Plaintiff Wikimedia Foundation, a non-profit organization based in San Francisco, California, operates several "wiki"-based projects and provides the contents of those projects to individuals around the world free of charge. Defendant National Security Agency/Central Security Service ("NSA") is the U.S. government agency responsible for conducting the surveillance at issue in this case. Defendant Office of the Director of National Intelligence ("ODNI") is the agency responsible for directing the activities of the U.S. intelligence community, including the NSA, and defendant Department of Justice ("DOJ") is one of the government agencies responsible for overseeing electronic surveillance. Several individual defendants are also named in their official capacities, including the Director of the NSA and the Chief of the Central Security Service, the Director of National Intelligence, and the Attorney General of the United States.

On June 22, 2015, plaintiff, along with eight other organizations,[3] filed the Amended Complaint in this suit, challenging the legality of defendants' Upstream surveillance program pursuant to § 702 of the FAA. The Amended Complaint alleges that this program violates (i) the Administrative Procedure Act ("APA"), (ii) the Fourth Amendment to the Constitution, (iii) the First Amendment to the Constitution, and (iv) Article III of the Constitution. The Amended Complaint seeks (i) a declaration that Upstream surveillance violates the APA and the Constitution and (ii) an injunction permanently enjoining defendants from continuing Upstream surveillance.

On August 6, 2015, defendants filed a Motion to Dismiss pursuant to Rule 12(b)(1), Fed. R. Civ. P., arguing that none of the plaintiff organizations plausibly alleged that they were injured by the interception, copying and review of online communications via the Upstream surveillance program and thus plaintiffs lacked Article III standing to contest the legality of the program. Subsequently, on October 23, 2015, an Order and a Memorandum Opinion issued, concluding that the allegations in the Amended Complaint were too speculative to establish Article III standing and granting defendants' motion to dismiss as to all plaintiffs. *See Wikimedia Found., et al., v. Nat'l Sec. Agency*, 143 F. Supp. 3d 344, 356-57 (D. Md. 2015), *aff'd in part, vacated in part, and remanded by* 857 F.3d 193 (4th Cir. 2017). Thereafter, plaintiffs appealed and the Fourth Circuit issued an opinion affirming in part, vacating in part, and remanding the case to the district court for further consideration. *See Wikimedia Found., et al., v. Nat'l Sec. Agency*, 857 F.3d 193 (4th Cir. 2017). Specifically, the Fourth Circuit concluded that although the eight other organizations had failed to allege injuries sufficient to satisfy the requirements of Article III standing, Wikimedia Foundation had alleged facts "sufficient to make plausible the conclusion that the NSA is

[3] These original plaintiffs included the National Association of Criminal Defense Lawyers, Human Rights Watch, Amnesty International USA, Pen American Center, Global Fund for Women, the Nation magazine, the Rutherford Institute, and the Washington Office on Latin America.

intercepting, copying, and reviewing at least some of Wikimedia's communications." *Wikimedia Found, et al..*, 857 F.3d at 210.

Shortly after the Fourth Circuit remanded the case to the district court for further proceedings, the parties submitted briefs on how to proceed in the case. Defendants indicated their intent to continue to challenge plaintiff's Article III standing and argued that any discovery should be bifurcated to allow for resolution of the standing question prior to resolution of the merits. Plaintiff opposed defendants' proposed discovery plan, contending that the jurisdictional facts at issue here are so intertwined with the merits as to require simultaneous discovery and summary judgment briefing on both questions. On October 3, 2017, an Order issued, directing the parties to conduct a limited five-month period of jurisdictional discovery prior to full discovery on the merits. *See Wikimedia Found. v. Nat'l Sec. Agency*, 1:15-cv-662 (D. Md. Oct. 3, 2017) (Order).

The parties then proceeded to engage in the limited discovery as directed. Plaintiff served 84 requests for admission, interrogatories, and requests for production on defendants, seeking what plaintiff describes as three broad categories of information: (i) direct evidence that Wikimedia has been surveilled, (ii) definition of key terms used in describing Upstream surveillance to the public, and (iii) evidence concerning the scope and breadth of Upstream surveillance.[4] Defendants responded to several of these discovery requests by producing 500 pages of unclassified documents, but objected to 53 of plaintiff's requests on the basis of privilege. In particular, defendants asserted that the information sought by plaintiff was protected by the common law state secrets privilege and other statutory privileges regarding the protection of national security information. In this respect, defendants submitted the unclassified declaration of Daniel Coats, the Director of National Intelligence, formally invoking the state secrets privilege on the basis of

[4] That these interrogatories covered both standing and merits matters is neither inappropriate nor unexpected, as these matters may well be inextricably entwined.

his personal consideration of the risks associated with disclosure of the information plaintiff seeks. Defendants also submitted a classified declaration of George C. Barnes, the Deputy Director of the NSA, providing additional detail concerning the harm to national security that would be caused by disclosure of the information contained in plaintiff's discovery requests.

Subsequently, on March 26, 2018, plaintiff filed the Motion to Compel at issue here pursuant to Rule 37(a)(3), Fed. R. Civ. P. Plaintiff contends that where, as here, a party moves to discover material relating to electronic surveillance, the court must follow FISA's § 1806(f) procedures and conduct an *ex parte* and *in camera* review of the materials relating to electronic surveillance. Plaintiff argues that these procedures apply despite defendants' assertion of state secrets privilege because in enacting FISA, Congress intended to displace the common law state secrets privilege. And even assuming the state secrets privilege was not displaced by FISA, plaintiff argues that the privilege does not bar disclosure of the information at issue here given the amount of information concerning Upstream surveillance already in the public record.

Defendants oppose plaintiff's motion, arguing (i) that § 1806(f) does not apply where, as here, plaintiff has not yet established that it is the target of electronic surveillance and (ii) that even assuming § 1806(f) does apply here, there is no clear statement indicating Congress's intent to displace the common law state secrets privilege through enactment of FISA. Finally, defendants contend that the government's assessment of the national security risks associated with disclosure of the information concerning plaintiff's discovery requests is entitled to deference and that plaintiff's arguments to the contrary are baseless.

III.

A threshold question that must be addressed is whether the *ex parte* and *in camera* review procedures established in § 1806(f) apply where, as here, a plaintiff is seeking classified discovery

to establish that the plaintiff's communications were unlawfully seized and searched. Analysis of this question properly begins with the terms of that statute. Section 1806(f) provides, in pertinent part:

> Whenever a court or other authority is notified pursuant to subsection (c) or (d) of this section, or whenever a motion is made pursuant to subsection (e) of this section, or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States . . . to discover or obtain applications or orders or other materials relating to electronic surveillance . . . the United States district court . . . shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

50 U.S.C. § 1806(f). The statute further defines "aggrieved person" as "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance." *Id.* § 1801(k).

This statutory text points persuasively to the conclusion that § 1806(f) procedures do not apply where, as here, a plaintiff has not yet established that it has been the subject of electronic surveillance. Specifically, the text of § 1806(f) identifies only three circumstances in which its procedures apply: (i) when the government notifies the court that it plans to introduce evidence obtained through electronic surveillance, (ii) when an aggrieved person moves to suppress information obtained through electronic surveillance, and (iii) when an aggrieved person makes "any motion or request . . . pursuant to any other statute or rule of the United States . . . to discover or obtain . . . materials relating to electronic surveillance." *Id.* Here, (i) and (ii) are clearly not met. The government has not noticed its intent to use or disclose information obtained through electronic surveillance, and plaintiff has not filed a motion to suppress any such information.

Accordingly, the only possible § 1806(f) situation applicable here is (iii), the third circumstance that may trigger § 1806(f). But importantly, § 1806(f) provides that this third situation applies only when the motion or request at issue "is made by an *aggrieved person*[,]"[5] namely "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance."[6] In this regard, the text of § 1806(f) makes clear that a party's status as an "aggrieved person," or the subject of surveillance, is a precondition to the application of § 1806(f)'s procedures; unless and until a party has adduced evidence that it has been the subject of electronic surveillance, a party's motion cannot trigger § 1806(f)'s *ex parte* and *in camera* review procedures.

This interpretation of the text is confirmed by the nature of § 1806(f)'s procedures once invoked. Specifically, § 1806(f)'s procedures require courts to engage in *ex parte* and *in camera* review of orders or other materials relating to surveillance to determine whether the surveillance at issue "was lawfully authorized and conducted." *Id.* § 1806(f). A determination that surveillance was lawfully authorized and conducted cannot occur unless a determination has previously been made that the surveillance at issue did, in fact, occur. Put differently, it is impossible to determine the lawfulness of surveillance if no surveillance has actually occurred. Thus, the text of § 1806(f) points persuasively to the conclusion that Congress intended § 1806(f) procedures to apply only after it became clear from the factual record that the movant was the subject of electronic surveillance.

Had Congress instead intended § 1806(f) to be a vehicle for parties to determine whether they were the target of electronic surveillance, one would expect to see language requiring courts

---

[5] *Id.*

[6] *Id.* § 1801(k).

to review materials relating to electronic surveillance to determine whether "electronic surveillance occurred," or requiring the government to affirm or deny the existence of any surveillance. Indeed, Congress has used precisely this language elsewhere in the U.S. Code. Specifically 18 U.S.C. § 3504, which was enacted eight years prior to FISA in 1970, provides that where a party claims evidence is admissible because the evidence is the product of an unlawful act, such as warrantless wiretapping, "the opponent of the claim shall affirm or deny the occurrence of the alleged unlawful act[.]" 18 U.S.C. § 3504. This provision demonstrates that Congress knew how to draft language requiring the government to affirm or deny the existence of some fact when Congress sought to do so. But importantly, § 1806(f) does not adopt this or similar language requiring an affirmation or denial of the fact of surveillance upon motion by an aggrieved person; rather, § 1806(f) provides that, upon a motion made by an aggrieved party, the court will determine whether the surveillance "was lawfully authorized and conducted." To assign meaning to this textual variation demands that § 1806(f) be interpreted to require *ex parte* and *in camera* review of the lawfulness of surveillance only after the individual has adduced evidence that he has been the target of electronic surveillance. *Cf. Lorillard v. Pons*, 434 U.S. 575, 584 (1978) (finding that Congress did not intend to apply the standards from one statute to a later-enacted statute where significant differences existed in the text of the two statutes).

Consideration of the other circumstances in which § 1806(f) procedures apply further bolsters the conclusion reached here. It is axiomatic that where, as here, "general words follow specific words in a statutory enumeration, the general words are usually construed to embrace only objects similar in nature to those objects enumerated by the preceding specific words." *Yates v. United States*, 135 S.Ct. 1074 (2015) (quoting *Washington State Dept. of Social & Health Servs. v. Guardianship Estate of Keffeler*, 537 U.S. 371, 384 (2003) (internal quotation marks omitted)).

In *Begay v. United States*, 553 U.S. 137, 142-43 (2008), the Supreme Court relied on this principle to determine whether specific crimes were covered by the statutory phrase "any crime . . . that . . . is burglary, arson, or extortion, involves use of explosives, or otherwise involves conduct that presents a serious potential risk of physical injury to another[.]" The Supreme Court reasoned that the enumeration of specific crimes—that is, burglary, arson, extortion, and use of explosives—indicated that the broadly worded "otherwise involves" provision covered "only similar crimes, rather than every crime that 'presents a serious potential risk of physical injury to another.'" *Id.* at 142.

The statutory provision at issue here—§ 1806(f)—is structured in precisely the same way as the provision at issue in *Begay*. Specifically, like the provision at issue in *Bergay*, § 1806(f) enumerates two specific situations covered by its procedures—namely, when the government provides notice pursuant to § 1806(c)-(d) and when a person against whom evidence is to be introduced moves to suppress that evidence pursuant to § 1806(e)—followed by a broadly-worded more general provision that also triggers § 1806(f)—namely, "whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States . . . to discover or obtain applications or orders or other materials relating to electronic surveillance . . . ." *Id.* As in *Bergay*, this broadly-worded, more general provision must be interpreted in light of the specifically enumerated provisions listed before it. And importantly, in each of these two specific situations, there is clear evidence that electronic surveillance has occurred; the only question is whether the evidence derived from the electronic surveillance may properly be disclosed.[7] Thus,

[7] This common thread uniting the situations in which § 1806(f) applies is further highlighted by the legislative history of this provision. Specifically, the Senate Report notes additional examples of instances in which § 1806(f)'s procedures apply, including "whenever an individual makes a motion pursuant to . . . 18 U.S.C. § 3504 . . . to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance . . . ." S. Rep. 95-701, 63, 1978 U.S.C.C.A.N. 3973, 4032. In this respect, the Senate Report explained that a defendant could "quer[y] the

to "avoid ascribing to one word a meaning so broad that it is inconsistent with its accompanying words" and to avoid "giving unintended breadth to the Acts of Congress[,]" it is necessary to interpret the final provision of § 1806(f) as similarly requiring evidence of the fact of electronic surveillance. *Gustafson v. Alloyd Co.*, 513 U. S. 561, 575 (1995).

Support for the conclusion reached here is found not solely in the text of § 1806(f) itself, but also in the caption of § 1806 and the general structure of the provision. Although "headings are not commanding," the Supreme Court has recognized that headings can "supply cues" that Congress did not intend a particular meaning of the statute. *Yates v. United States*, 135 S. Ct. 1074, 1083 (2015). Section 1806's heading—use of information—suggests that Congress did not intend §1806(f) to apply in situations where, as here, it is yet unclear whether electronic surveillance even occurred. Rather, the heading suggests that Congress intended the provisions of § 1806 to apply where evidence already establishes the fact of surveillance, and the central dispute is instead how, and whether, information obtained via that electronic surveillance can be used or disclosed in a proceeding.

Finally, as the Supreme Court has recognized, "[i]t is axiomatic that statutes in derogation of the common law should be narrowly construed[.]" *Badaracco v. C.I.R.*, 464 U.S. 386, 403 n.3 (1984). In this case, as plaintiff notes, § 1806(f) seems on its face to conflict with traditional principles of common law, namely the common law state secrets privilege. Specifically, the mandatory *ex parte* and *in camera* review procedures established in § 1806(f), in situations in which these procedures apply, likely displace the common law process whereby courts review the government's assertion of the state secrets privilege to avoid disclosure of information potentially harmful to national security. Given this, traditional principles of statutory interpretation counsel

government under 18 U.S.C. § 3504," "discover[] that he has been intercepted by electronic surveillance" and then move to suppress or to discover or obtain information related to that surveillance.

that FISA must be narrowly construed so as to avoid excessive displacement inconsistent with Congress's intent. To interpret the text of § 1806(f) broadly, as plaintiff here suggests, to encompass not just motions raised by parties who have adduced evidence that they are "aggrieved persons," but also motions by parties who simply allege that they are "aggrieved persons," would do precisely this, namely displace the common law to an extent neither contemplated nor intended by Congress.

In an attempt to avoid this conclusion, plaintiff contends that the allegations contained in the complaint are sufficient to establish that plaintiff is an "aggrieved person" within the meaning of § 1806(f). Specifically, defendant cites to the Fourth Circuit's determination that plaintiff's complaint alleges sufficient facts "to make plausible the conclusion that the NSA is intercepting, copying, and reviewing at least some of [plaintiff's] communications" and contends that this plausibility determination is sufficient standing alone to require invocation of § 1806(f)'s procedures. *Wikimedia Found., et al.*, 857 F.3d at 211. But the Fourth Circuit concluded that plaintiff had sufficiently alleged injury-in-fact for the purposes of surviving a motion to dismiss; the Fourth Circuit never considered the requisite showing of "aggrieved person" status to trigger the earlier procedures outlined in § 1806(f). *Id.* at 207-11. As such, the Fourth Circuit's determination in *Wikimedia* does not answer the question raised here—namely what showing is required prior to invocation of § 1806(f) procedures.

Notably, the only circuit authority to consider this latter question—what a party must show to establish his or her "aggrieved person" status and invoke § 1806(f)—recognized that a party may not trigger § 1806(f) procedures unless and until the party has adduced evidence of its "aggrieved person" status. Specifically, in *ACLU Foundation of Southern California v. Barr*, 952 F.2d 457 (D.C. Cir. 1991), the D.C. Circuit reversed the district court's dismissal of the plaintiffs'

First Amendment claim based on the government's surveillance of plaintiffs' communications. In denying the motion to dismiss, the D.C. Circuit reasoned that "legitimate concerns about compromising ongoing foreign intelligence investigations" are more properly considered at the summary judgment stage, not upon the pleadings. *Id.* at 469. In this respect, the D.C. Circuit explained that plaintiffs challenging alleged unlawful electronic surveillance must survive summary judgment—that is, they must adduce evidence sufficient to prove the existence of a genuine dispute about the fact of ongoing surveillance before the court applies § 1806(f) procedures. *Id.* The D.C. Circuit recognized that "in the usual case some discovery is permitted before the court rules on a motion for summary judgment," but importantly, the D.C. Circuit noted that "normal rules regarding discovery must be harmonized with FISA and its procedures, notably 1806(f)." *Id.* In this regard, The D.C. Circuit further explained that:

> even plaintiffs who defeat summary judgment motions would not be entitled to obtain any of the materials relating to the authorization of the surveillance or the evidence derived from it unless the district court, in an *ex parte, in camera* proceeding, first determined that the surveillance was not "lawfully authorized and conducted."

Id. This analysis in *Barr* makes clear that the D.C. Circuit contemplated the conclusion reached here, namely that in order to trigger § 1806(f) procedures, a plaintiff must first adduce evidence sufficient at least to create a genuine dispute as to whether the plaintiff has been the target of electronic surveillance in the past or whether electronic surveillance is ongoing.

Plaintiff next argues that to require a plaintiff to adduce evidence of surveillance to demonstrate his or her "aggrieved person" status would necessarily mean that a plaintiff could not do so unless the government affirmatively acknowledges the fact of surveillance. And to require the government affirmatively to acknowledge the fact of surveillance prior to invocation of § 1806(f) procedures, plaintiffs contend, would be inconsistent with other provisions in the statute, namely the civil cause of action established in § 1810.

This argument fails to persuade because it mischaracterizes both (i) the requirements for establishing "aggrieved person" status and (ii) the nature of the civil remedy established in § 1810. To begin with, affirmative government acknowledgement of surveillance of a specific target is not the only means by which a plaintiff can establish evidence of his or her "aggrieved person" status. Indeed, courts have recognized that plaintiffs can "rely on many non-classified materials, including present and future public disclosures of the government or [telecommunications providers] on the alleged NSA programs" to establish that they have been the target of electronic surveillance. *Hepting v. AT&T Corp., et al.*, 439 F. Supp. 2d 974, 998 (N.D. Cal. 2006). Thus, to require a plaintiff to adduce evidence of surveillance to demonstrate his or her "aggrieved person" status does not necessarily require that the government affirmatively acknowledge the fact of surveillance.

And even assuming, *arguendo*, that affirmative government acknowledgment was the only means by which a plaintiff could prove his or her "aggrieved person" status, this requirement would not be inconsistent with the remedy established in § 1810. That section provides a civil remedy to "[a]n aggrieved person . . . who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 1809." 50 U.S.C. § 1810. Plaintiff argues that to require government acknowledgement of surveillance prior to invocation of § 1806(f) procedures would render § 1810 a nullity because plaintiff's access to the remedy against the government would be dependent entirely on cooperation by the government. This argument is unpersuasive; courts have made clear that § 1810 is not actually a remedy against the government because § 1810 does not contain an explicit waiver of sovereign immunity. *See Al-Haramain Islamic Found., Inc. v. Obama*, 705 F.3d

845, 854 (9th Cir. 2012).[8] Instead, § 1810 provides a remedy against intelligence agents who engage in unlawful electronic surveillance or who disclose information obtained from unlawful surveillance in their personal, not official, capacities. In this respect, the civil cause of action in § 1810 is premised upon the individual agent's "violation of section 1809[,]" which establishes criminal penalties for unlawful surveillance. *Al-Haramain*, 705 F.3d at 854 (quoting 50 U.S.C. 1810).[9] There is no reason to believe that the government would be unwilling to cooperate in acknowledging that an individual agent conducted unlawful surveillance in his individual capacity. Indeed, to the extent that § 1810 is intended to track an individual agent's criminal liability, the government will necessarily acknowledge, and indeed prove, the fact of surveillance through a criminal prosecution of that individual agent.

Finally, plaintiff cites to one case in which a district court found that the plaintiffs "alleged enough to plead 'aggrieved person' status so as to proceed to the next step in proceedings under FISA sections 1806(f) and 1810." *In re NSA Telecommc'ns Records Litig.*, 595 F.Supp.2d 1077, 1085-86 (N.D. Cal. 2009). But in reaching this conclusion—namely that the allegations in plaintiff's complaint were sufficient to invoke § 1806(f) procedures—the court did not conduct an in-depth analysis of the text or indeed even of the legislative history of FISA. Instead, the *In re NSA Telecommunications Records Litigation* court imported a standard from the Ninth Circuit's analysis of claims pursuant 18 U.S.C. § 3504.[10] Section 3504 provides, in relevant part, that "upon a claim by a party aggrieved that evidence is inadmissible because it is the primary product of an

---

[8] *See also Whitaker v. Barksdale Air Force Base*, 2015 WL 574697, *7 (W.D. La. Feb. 11, 2015) (agreeing with the "extensive analysis" in *Al-Haramain*).

[9] *See also* H.R. Conf. Rep. No. 95-1720 (noting that the cause of action in § 1810 is afforded "to any aggrieved person about whom information has been disclosed or used in violation of the criminal penalty provisions" and that "civil liability of intelligence agents under this act should coincide with the criminal liability.").

[10] 18 U.S.C. 3504

unlawful act . . . , the opponent of the claim shall affirm or deny the occurrence of the alleged unlawful act." 18 U.S.C. § 3504. In *United States v. Alter*, 482 F.2d 1016 (9th Cir. 1974), the Ninth Circuit concluded that § 3504's requirement to affirm or deny the occurrence of the alleged unlawful act is triggered where the party aggrieved makes a "prima facie showing that good cause exists to believe" the individual was subject to illegal surveillance. *Id.* at 1026.

Plaintiff's reliance on *In re NSA Telecommunications Records Litigation* and its application of the § 3504 standard in the FISA context is unpersuasive because § 3504 is different from § 1806(f) in significant ways. Notably, although both § 1806(f) and § 3504 use the term "aggrieved," § 1806(f), unlike § 3504, incorporates a statutory definition of an "aggrieved person," which specifies that an "aggrieved person" is "a person who is the target of an electronic surveillance" or "whose communications or activities were subject to surveillance[.]" 50 U.S.C. § 1801(k). As such, while a party can claim to be aggrieved for the purposes of § 3504 through a "mere assertion"[11] that unlawful surveillance has occurred, § 1806(f) requires that the person has actually been a target of electronic surveillance or has been subject to surveillance before that individual can trigger the *ex parte* and *in camera* review procedures outlined in § 1806(f).

Moreover, the reasoning in support of the low burden in the § 3504 context does not apply here. Specifically, in analyzing § 3504, courts have reasoned that the government's obligation to affirm or deny the occurrence of unlawful surveillance is triggered by the mere assertion of unlawful wiretapping because "requiring the government to affirm or deny the existence of illegal surveillance of witnesses imposes only a minimal additional burden upon the government." *Vielguth*, 502 F.2d at 1259 n.4 (citing *In re Evans*, 452 F.2d at 1247). But this reasoning is inapplicable here because § 1806(f) requires much more than a simple affirmation or denial by the

[11] *United States v. Vielghth*, 502 F.2d 1257, 1258 (9th Cir. 1974) (quoting *In re Evans*, 452 F.2d 1239, 1247 (1971)).

government. Section 1806(f) procedures, once triggered, require the court to review *ex parte* and *in camera* all of the relevant materials relating to electronic surveillance—in this case, potentially 10,000 pages of documents—to determine the lawfulness of the surveillance. The reasoning justifying the low burden in § 3504 is thus inapplicable here where a much higher burden is associated with the applicable procedures. Given that the *In re NSA Telecommunications Records Litigation* court, in interpreting the requirements of § 1806(f), relied on a standard imported from 18 U.S.C. § 3504, which, for the reasons described above, is inapplicable here, plaintiff's reliance on *In Re NSA Telecommunications Records Litigation* is unpersuasive and does not alter the conclusion reached here.[12]

In sum, when interpreted in light of traditional principles of statutory interpretation, the text of § 1806(f) makes clear that § 1806(f) procedures do not apply where, as here, the plaintiff has merely plausibly alleged that it has been the target of surveillance and has not yet adduced evidence establishing this fact of surveillance. Accordingly, it is not appropriate at this time to engage in *ex parte* and *in camera* review of the materials responsive to plaintiff's interrogatories or to those plaintiff describes in its motion to compel.

IV.

---

[12] It is also worth noting that despite the *In re NSA Telecommunications Records Litigation* court's determination that the plaintiffs there had sufficiently alleged their aggrieved person status, the court nonetheless declined to follow the mandatory § 1806(f) procedures. 595 F.Supp.2d at 1086-90. Specifically, the court ordered the government to produce responsive materials, but has yet to make a finding as to the lawfulness of any surveillance and has not provided the plaintiffs access to any discovery materials. *Id.*

Plaintiff also cites to *Jewel v. NSA*, a Northern District of California case in which the district court issued several orders, directing the government to produce materials for *ex parte* and *in camera* review. But the *Jewel* court appeared not to address the requisite showing of "aggrieved person" status, and as such, that case did not directly address the issues addressed here. Indeed, the *Jewel* court has not yet issued an order as to the lawfulness of any alleged surveillance in that case and has recently issued an order requesting additional briefing on how plaintiffs can "establish they may be aggrieved persons without access to [classified] information" and "the current legal standard for asserting standing in these circumstances." *Jewel v. NSA*, No. 08-cv-4373, at *1 (N.D. Cal. July 5, 2018). As such, it is clear that the *Jewel* court has not yet definitively resolved the issues addressed here.

Given that § 1806(f) procedures do not apply here, it is unnecessary to consider the question whether § 1806(f) displaces the state secrets privilege in situations in which § 1806(f) does apply. As such, the only remaining question is whether the government's invocation of the state secrets privilege defeats plaintiff's motion to compel.

A.

It is necessary first to review the well-settled Supreme Court and Fourth Circuit precedents governing the assertion of the state secrets privilege. Supreme Court and Fourth Circuit precedent make clear that "[u]nder the state secrets doctrine, the United States may prevent the disclosure of information in a judicial proceeding if 'there is a reasonable danger' that such disclosure 'will expose . . . matters which, in the interest of national security should not be divulged." *Abilt v. CIA*, 848 F.3d 305, 310-11 (4th Cir. 2017) (quoting *El-Masri v. United States*, 479 F.3d 296, 302 (4th Cir. 2007) (quoting *United States v. Reynolds*, 345 U.S. 1, 10 (1953)). In this regard, the Fourth Circuit has recognized that the state secrets privilege "performs a function of constitutional significance, because it allows the executive branch to protect information whose secrecy is necessary to its military and foreign-affairs responsibilities." *Id.* at 312 (quoting *El–Masri*, 479 F.3d at 303).

The Fourth Circuit has mandated a three-step analysis for resolution of a state secrets question:

> First, "the court must ascertain that the procedural requirements for invoking the state secrets privilege have been satisfied." Second, "the court must decide whether the information sought to be protected qualifies as privileged under the state secrets doctrine." Third, if the "information is determined to be privileged, the ultimate question to be resolved is how the matter should proceed in light of the successful privilege claim."

Albit, 848 F.3d at 311 (quoting *El-Masri*, 479 F.3d at 304).

With respect to the first step in this analysis, the Supreme Court has specified three procedural requirements for invocation of the state secrets privilege: (i) the state secrets privilege must be asserted by the United States government; it "can neither be claimed nor waived by a private party," (ii) "[t]here must be a formal claim of privilege, lodged by the head of the department which has control over the matter," and (iii) the department head's formal claim of the state secrets privilege must be made only "after actual personal consideration by that officer." *Reynolds*, 345 U.S. at 7-8 (footnotes omitted). If these procedural requirements are satisfied, the court may proceed to the second step of the analysis.

This second step of the analysis requires courts to "determine whether the information that the United States seeks to shield is a state secret, and thus privileged from disclosure." *El-Masri*, 479 F.3d at 304. In this respect, courts must "assure [themselves] that an appropriate balance is struck between protecting national security matters and preserving an open court system." *Albit*, 848 F.3d at 311-12 (quoting *Al-Haramain Islamic Found., Inc. v. Bush*, 507 F.3d 1190, 1203 (9th Cir. 2007)). That is, courts assessing a claim of state secrets privilege must simultaneously accord "utmost deference"[13] to the Executive Branch's assessment of the risk to national security posed by the disclosure of information while also "critically examin[ing] instances of [the privilege's] invocation" so as "not to accept at face value the government's claim or justification of privilege."[14]

The Supreme Court has balanced these competing concerns by requiring courts to determine "from all the circumstances of the case, [whether] there is a reasonable danger that compulsion of the evidence will expose . . . matters which, in the interest of national security,

---

[13] *Albit*, 848 F.3d at 312 (quoting *United States v. Nixon*, 418 U.S. 683, 710 (1974), *superseded by statute on other grounds as recognized by Bourjaily v. United States*, 483 U.S. 171, 177-79 (1987)).

[14] *Id.* at 312 (quoting *Al-Haramain*, 507 F.3d at 1203; *Ellsberg v. Mitchell*, 709 F.2d 51, 58 (D.C. Cir. 1983)).

should not be divulged.'" *Reynolds*, 345 U.S. at 10. The government bears the burden of satisfying "the reviewing court that the *Reynolds* reasonable-danger standard is met." *Albit*, 848 F.3d at 312 (quoting *El-Masri*, 479 F.3d at 305). In this regard, the Fourth Circuit has recognized that the explanation proffered by the department head who formally invokes the privilege is "frequently . . . sufficient to carry the Executive's burden." *Id.* (quoting *El-Masri*, 469 F.3d at 305). In the end, if the government carries its burden and shows that there is a reasonable danger that disclosure of information will expose matters that should not be divulged, "court[s] [are] obliged to honor the Executive's assertion of the privilege[.]" *Id.* (quoting *El-Masri*, 479 F.3d at 305).

If the procedural requirements for invocation of the state secrets privilege are satisfied and the court determines that the information sought to be disclosed is properly privileged, the final step in the analysis is to assess how the matter should proceed. Here, again, Fourth Circuit and Supreme Court precedent is clear: if the state secrets privilege has been successfully invoked, "the claim of privilege will be accepted without requiring further disclosure." *Id.* (quoting *Reynolds*, 345 U.S. at 9).

B.

With these principles in mind, it is appropriate now to consider the assertion of the state secrets privilege in this case. To begin with, the procedural requirements for invocation of the state secrets privilege have been satisfied.[15] Defendants, the NSA, ODNI, and the DOJ, are U.S. government agencies and thus can properly claim the state secrets privilege. The claim of privilege was lodged by Daniel Coats ("Coats"), the Director of National Intelligence ("DNI"), who is the head of the U.S. Intelligence Community and in this regard, is tasked with the protection of

[15] Indeed, Wikimedia does not appear to dispute this point.

intelligence sources and methods from unauthorized disclosure. *See* Coats Decl. ¶ 1.[16] Finally, Coats invoked the privilege formally after personally considering the nature of plaintiff's discovery requests and determining that disclosure of the information requested reasonably could be expected to cause exceptionally grave damage, and at the very least, serious damage, to U.S. national security. *See* Coats Decl. ¶¶ 6, 16, 24, 28, 32, 35, 39, 43. Accordingly, it is clear that defendants have satisfied the procedural requirements for invocation of the state secrets privilege.

The government has similarly satisfied its burden with respect to the second step of the state secrets privilege analysis as careful review of the public Coats declaration and the classified Barnes declaration reveals that "there is a reasonable danger that compulsion of the evidence will expose . . . matters which, in the interest of national security, should not be divulged." *Reynolds*, 345 U.S. at 10. Specifically, through public and classified declarations defendants have identified seven categories of information covered by plaintiff's discovery requests, including: (i) entities subject to Upstream surveillance activities, (ii) operational details of the Upstream collection process, (iii) locations at which Upstream surveillance is conducted, (iv) categories of Internet-based communications subject to Upstream surveillance activities, (v) the scope and scale on which Upstream surveillance is or has been conducted, (vi) NSA's cryptanalytic capabilities, and (vii) additional categories in contained in FISC opinions and submissions. Moreover, defendants have provided detailed descriptions, in more than 60 pages of classified declarations, explaining that disclosure of these categories of information would undermine ongoing intelligence operations, deprive the NSA of existing intelligence methods, and significantly, provide foreign adversaries with the tools necessary both to evade U.S. intelligence operations and to conduct their

[16] *See also* 50 U.S.C. § 3024(i)(1) (providing that "[t]he Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure.").

own operations against the United States and its allies. In sum, it is clear that there is a reasonable, and indeed likely, danger that disclosure of this information will expose matters which should not be divulged in the interest of national security, and as such, this information falls squarely within the ambit of the state secrets privilege. *See, e.g.*, *Albit*, 848 F.3d at 314 (concluding that "[t]here is little doubt that there is a reasonable danger that if information . . . regarding . . . the sources and methods used by the CIA [and] the targets of CIA intelligence collection and operations . . . were revealed, that disclosure would threaten the national security of the United States").[17]

In an attempt to avoid this conclusion, plaintiff contends that to acknowledge the fact that plaintiff has been subject to surveillance would not, in fact, threaten national security. This argument plainly fails because courts have concluded that where, as here, the information sought to be disclosed involves the identity of parties whose communications have been acquired, this information is properly privileged. *See* Al-*Haramain*, 507 F.3d at 1203-04 (finding that the fact of a plaintiff's surveillance by the NSA was covered by the state secrets privilege); *Halkin v. Helms*, 598 F.2d 1, 9 (D.C. Cir. 1978) (upholding assertion of state secrets privilege with respect to "the identity of particular individuals whose communications have been acquired").

Plaintiff contends that, contrary to surveillance of a particular individual with limited communications, plaintiff's communications are so ubiquitous that to reveal surveillance of its communications would not provide information regarding the structure of the Upstream surveillance program or its specific targets. Although this proposition may appear to have some force, courts have consistently recognized that "judicial intuition" about a proposition such as this

---

[17] *See also, e.g.*, *Sterling v. Tenet*, 416 F.3d 338, 342 (4th Cir. 2005) ("There is no question that information that would result in . . . disclosure of intelligence-gathering methods or capabilities . . . falls squarely within the definition of state secrets." (quoting *Molerio v. FBI*, 749 F.2d 815, 820-21 (D.C. Cir. 1984) (internal quotation marks omitted)); *Jewel v. NSA*, 2015 WL 545925, at *5 (N.D. Cal. Feb. 10, 2015) (finding "[d]isclosure of this classified information would risk informing adversaries of the specific nature and operational details of the Upstream collection process").

"is no substitute for documented risks and threats posed by the potential disclosure of national security information." *Al-Haramain*, 507 F.3d at 1203. And defendants have thoroughly documented those risks in the classified declaration here, explaining that to reveal the fact of surveillance of an organization such as plaintiff, even considering plaintiff's voluminous online communications, would provide insight into the structure and operations of the Upstream surveillance program and in so doing, undermine the effectiveness of this intelligence method.

Finally, plaintiff argues that there cannot be a reasonable danger of undermining national security because much of the information plaintiff seeks is already contained in publicly-accessible documents. But importantly, the information disclosed in these public documents is plainly different from the information that plaintiff seeks. For example, plaintiff's requests for admissions 13 through 15 ask defendants to admit that the NSA is conducting Upstream surveillance via "multiple INTERNET BACKBONE CIRCUITS," "multiple international Internet link[s]," and "multiple INTERNET BACKBONE 'chokepoints.'" Plaintiff contends that these facts have already been acknowledged by the NSA, as reflected in the PCLOB Report and certain unclassified portions of FISC opinions. Specifically, plaintiff contends that the PCLOB report's reference to "circuits" suggests the NSA is conducting surveillance on more than one circuit. To be sure, the PCLOB report does use the term "circuits," but it does not do so to refer to the number of sites the NSA is monitoring. Instead, the PCLOB report uses the term "circuits" in the context of defining the "Internet backbone." Specifically, the PCLOB report explains that the "Internet backbone" consists of "circuits that are used to facilitate Internet communications[.]" PCLOB Rep. at 36. Similarly, the redacted FISC Opinion cited by plaintiff does not, as plaintiff contends, confirm that the NSA is monitoring multiple international Internet links; instead, the redacted October 3, 2011 FISC Opinion states that "the government readily concedes that NSA will acquire a wholly

domestic 'about' communication if the transaction containing the communication is routed through an international Internet link being monitored by the NSA . . . ." 2011 WL 10945618, at *15 (FISC Oct. 3, 2011). Nothing in this statement confirms that the NSA is monitoring multiple internet links.[18] Ultimately, plaintiff's argument fails because although the government has declassified certain information about the Upstream surveillance program, the government has not yet released the precise information at issue here. Accordingly, this information is still properly subject to the state secrets privilege.

In sum, a careful review of defendants' public and classified declarations reveals (i) that defendants have satisfied the procedural requirements necessary to invoke the state secrets privilege and (ii) that the information sought to be protected qualifies as privileged under the state secrets doctrine. Given that defendants have satisfied the requirements of the state secrets privilege, "the claim of privilege will be accepted without requiring further disclosure." *Albit*, 848 F.3d at 31 (quoting *Reynolds*, 345 U.S. at 9). Accordingly, plaintiff's motion to compel must be denied.[19]

An appropriate Order will issue.

Alexandria, Virginia
August 20, 2018

/s/
T. S. Ellis, III
United States District Judge

[18] Plaintiff similarly argues that the fact that the NSA reviews the type of Internet communications in which plaintiff engages, namely HTTP and HTTPS Internet protocols, is available in the public record. But contrary to plaintiff's suggestion, the use of the general phrase "web activity" in an unclassified portion of the June 1, 2011 FISC Opinion does not confirm that the NSA is monitoring any specific Internet protocol, namely either HTTP or HTTPS.

[19] It is worth emphasizing the narrow scope of this decision, namely (i) that FISA § 1806 is not triggered in this case and that this provision and the associated FISA procedures do not operate here to displace the common law state secrets privilege and (ii) that the government has satisfied the well-settled procedural requirements necessary to invoke the privilege. Neither addressed nor resolved here is whether this long-ago judicially created privilege has, or should have, any continuing vitality today. That is not a question within the province of a district court.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION,	)	
Plaintiff,	)	
	)	
v.	)	**Case No. 1:15-cv-662**
	)	
NATIONAL SECURITY AGENCY/ CENTRAL SECURITY SERVICE, *et al.*,	)	
	)	
Defendants.	)	

ORDER

This matter came before the Court on plaintiff's Motion to Compel Discovery Responses and Deposition Testimony.

For the reasons stated in the accompanying Memorandum Opinion of even date,

It is hereby **ORDERED** that the motion is **DENIED**.

The Clerk is directed to provide a copy of this Order to all counsel of record.

Alexandria, Virginia
August 20, 2018

/s/
T. S. Ellis, III
United States District Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, Plaintiff, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	Civil Action No. 1:15-cv-00662-TSE

Attachment C

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, Plaintiff, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	Civil Action No. 1:15-cv-00662-TSE ~~FILED UNDER SEAL~~

EXHIBIT 1

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION,	)	
Plaintiff,	)	
v.	)	No. 1:15-cv-0662 (TSE)
NATIONAL SECURITY AGENCY, *et al.*,	)	
Defendants.	)	

DECLARATION OF DR. HENNING SCHULZRINNE

Dr. Henning Schulzrinne, for his declaration pursuant to 28 U.S.C. § 1746, deposes and says as follows:

INTRODUCTION

1. I am the Julian Clarence Levi Professor of Computer Science at Columbia University in New York, New York. I submit this declaration at the request of the United States Department of Justice to address technical issues surrounding, and to render opinions concerning, the assertion of plaintiff Wikimedia Foundation ("Wikimedia") that the National Security Agency ("NSA"), in the course of conducting electronic surveillance known as "Upstream" collection, must as a matter of technological necessity be intercepting, copying, and reviewing at least some of Wikimedia's electronic communications that traverse the Internet. For the reasons I detail herein, that assertion is incorrect. Based on what is publicly known about the NSA's Upstream collection technique, the NSA in theory could be conducting this activity, at least as Wikimedia conceives of it, in a number of ways that would not involve NSA interaction with Wikimedia's online communications.

2. A complete statement of my conclusions in this matter and the bases for them are set forth below, as are my background and qualifications in the fields of computer science, electrical engineering, and digital communications technology, and the sources of information I considered in arriving at the conclusions stated herein. I am being compensated for my services in this matter at the rate of $350 per hour. I have not previously testified as an expert whether by declaration, at trial, or by deposition.

QUALIFICATIONS

3. I received my Ph.D. in Electrical Engineering in 1992 from the University of Massachusetts at Amherst, a Master's Degree in Electrical Engineering as a Fulbright scholar at the University of Cincinnati, Ohio, in 1987, and undergraduate degrees in Electrical Engineering and Economics from the Darmstadt University of Technology (Technische Hochschule) in Darmstadt, Germany, in 1984.

4. Prior to joining the faculty at Columbia University, I was an associate department head, from 1994 to 1996, at the Fraunhofer Institute for Open Communication Systems in Berlin, Germany (FOKUS), formerly an institute of the Society for Mathematics and Data Processing (GMD). From 1992 to 1994 I was a member of the technical staff at AT&T Bell Laboratories in Murray Hill, New Jersey.

5. I joined the faculty at Columbia University as a Professor of Computer Science and Electrical Engineering (a dual appointment) in 1996, and was named as Julian Clarence Levi Professor of Computer Science in 2009. I chaired the Department of Computer Science from 2004 to 2009. I teach courses in Computer Networks; Advanced Internet Services; and Internet Technology, Economics, and Policy and have in the past taught courses on network security and advanced programming. Concurrent with my position on the faculty at Columbia, from 2010 to 2012 I was an Engineering Fellow and Technical Advisor at the Federal Communications Commission (FCC), and Chief Technology Officer of the FCC from 2012 to 2017. In that role I guided the FCC's work on technology and engineering issues to ensure that FCC policies promoted technological innovation in the telecommunications industry.

6. In addition to my teaching responsibilities, I also head Columbia University's Internet Real-Time Laboratory, which under my supervision conducts research in the areas of real-time Internet multimedia services and Internet telephony; wireless and mobile networks; streaming; quality of service; resource reservation; dynamic pricing for the Internet; network measurement and reliability; service location; network security; media on demand; content distribution networks; multicast networks and ubiquitous and context-aware computing and communication; and designs, analyses and prototypes for next-generation "radio," "TV," and "telephone" networks. Additional research interests of mine include Internet signaling, packet scheduling, multicast, the use and development of security algorithms and protocols for prevention of denial-of-service attacks, secure multimedia services, and resource reservations.

7. Over the course of my career in the field of digital communications technology I have co-developed a number of Internet protocols (or supervised their development at the Internet Real-Time Lab). Broadly speaking, Internet protocols are generally accepted sets of rules governing how different types of Internet communications are to be structured so that they may be efficiently transported on, and intelligibly sent and received by devices connected to, the Internet. A number of the protocols that I have developed are now used by almost all Internet telephony and multimedia applications. Among the most prominent are:

- Real-time Transport Protocol (RTP): a network protocol for transmitting audio and video services over Internet Protocol networks, used extensively in communication and entertainment systems that involve streaming media, such as telephony, video teleconferencing and television services.
- Real-Time Streaming Protocol (RTSP): a network control protocol designed for use in entertainment and communications systems to control (rather than transmit) streaming media services, allowing end users to issue VCR-style commands, such as *play*, *record* and *pause*, to facilitate real-time control of the media streaming
- Session Initiation Protocol (SIP): a signaling protocol used for initiating, maintaining, and terminating real-time multimedia communication sessions in applications of Internet telephony for voice and video calls, in private IP telephone systems, in instant messaging over Internet Protocol networks as well as mobile phone calling.

8. My current professional associations include the Institute of Electrical and Electronics Engineers (IEEE), of which I was named a Fellow in 2006 in recognition of my contributions to the design of protocols, applications, and algorithms for Internet multimedia. I have been a member of the Board of Governors of the IEEE Communications Society, past Chair of the IEEE Communications Society Technical Committee on Computer Communications, and past Co-Chair of the IEEE Communications Society Internet Technical Committee. I am also a member of the Association for Computing Machinery (ACM), and served as Vice Chair of ACM's Special Interest Group on Data Communications and the Internet (SIGCOMM).

9. I have also been a member of the Internet Architecture Board (IAB), a committee of the Internet Engineering Task Force (IETF) with responsibility for, among other matters, providing architectural oversight of Internet protocols and procedures, managing Internet standards documents (the "RFC" series) and protocol parameter value assignment. The IAB also acts as an advisory board to the Internet Society (ISOC), the internationally recognized body committed to the open development of Internet standards, protocols, and technical and administrative infrastructure. I also served on the Internet2 Applications, Middleware and Services Advisory Council and have led a working group in the National Science Foundation's GENI (Global Environment for Network Innovations) project, which provides a virtual laboratory for networking and distributed systems research and education.

10. I also serve on a number of conference and journal steering committees, including for the IEEE/ACM journal Transactions on Networking, a bi-monthly publication of high-quality papers that advance the state of the art in communication network research, including theoretical research presenting new techniques, concepts, or analyses, as well as applied contributions reporting on experiences and experiments with actual systems. In the past, I have chaired or co-chaired various IEEE and ACM annual global conferences in the field digital communications technology.

11. I have published more than 250 journal and conference papers, and more than 70 Internet RFCs. (RFCs are publications documenting Internet specifications, communications

protocols and procedures adopted as standards by the IETF, but from time to time are also informative in nature, describing research or innovations applicable to the working of the Internet and Internet-connected systems.) A list of my publications, including all publications I have authored in the previous 10 years, may be found in my curriculum vitae, a copy of which is attached to this declaration as Exhibit A. I have also been editor of several periodicals in the field of computer science, including "Computer Communications Journal," "ACM Transactions on Multimedia Computing," and "ComSoc Surveys & Tutorials," "IEEE Transactions on Image Processing," the "Journal of Communications and Networks," "IEEE/ACM Transactions on Networking," and "IEEE Internet Computing Magazine."

12. In 2013, I was inducted into ISOC's Internet Hall of Fame, in recognition of my contributions to the development of key Internet protocols, including the RTP, RTSP, and SIP protocols noted above. Among other awards, I received the New York City Mayor's Award for Excellence in Science and Technology, the VON Pioneer Award by the Voice-over-Net Conference, the IEEE Technical Committee on Computer Communications Outstanding Service Award, and the IEEE Region 1 William Terry Award for Lifetime Distinguished Service to the IEEE.

FACTS AND INFORMATION CONSIDERED

13. For purposes of preparing this declaration, I have relied on (and cite herein) various types of sources, including: (i) Internet standards documents adopted and published by the IETF, known as RFCs, *see* paragraph 11, above, available at https://www.rfc-editor.org/search/rfc_search.php; (ii) public registries and other websites where information concerning assigned protocol and port numbers, IP addresses, and the like, may be found; (iii) various publicly available statistics and technical information concerning Internet infrastructure; (iv) information obtained from manufacturer websites; (v) standard college textbooks, written by well-established leaders in the field, that have become the accepted teaching materials for engineering and computer science students entering the field of computer networks; and (vi) my own knowledge of and familiarity with the technology and operation of global communications networks.

14. As appropriate, I also refer to documents and information produced by Wikimedia in discovery proceedings in this case, and to official U.S. Government documents publicly describing, in unclassified terms, the operation of NSA Upstream surveillance. A list of the documents provided to me by Justice Department counsel, and which I have also reviewed, is attached as Exhibit B. In reaching the conclusions stated herein I have not considered nor have I been provided with any classified or other non-public information concerning the Upstream program.

SUMMARY OF CONCLUSIONS

15. Principally, I have been asked to evaluate Wikimedia's assertion that the NSA, in the course of conducting Upstream surveillance, must as a matter of technological necessity be intercepting, copying, and reviewing at least some of Wikimedia's electronic communications that traverse any Internet backbone "link" monitored by the NSA. For the reasons I explain at length below, I conclude that Wikimedia's assertion is incorrect. Based on what is publicly known about the NSA's Upstream collection technique, the NSA could be conducting Upstream-type surveillance, at least as envisioned by Wikimedia, in a number of technically feasible, readily implemented ways that would not involve NSA interaction with Wikimedia's online communications.

INTERNET INFRASTRUCTURE

16. Technically speaking, the Internet is a global collection of networks, large and small, "interconnected by a set of routers which allow them to function as a single, large virtual network." (RFC 1208, 1991) In other words, it is a network of networks, owned and operated by thousands of private and public entities across the world, including telecommunications service providers, governments, and non-profit organizations. There is no precise count of the number of networks that together make up the Internet, but currently there are approximately 62,000 autonomous systems (networks or collections of networks managed and supervised by large entities or organizations) with their own identifiers (Autonomous System Numbers) assigned by the global Internet Assigned Numbers Authority (IANA). These include networks operated by

Columbia University (AS 14), the Wikimedia Foundation (AS 14907), Google (AS 15169) and large carriers such as Verizon (AS 702 and others). Consisting of servers, communication links, and intermediate devices that route information from one network to another ("routers"), this infrastructure allows any device connected to this network of networks to send information to any other connected device (subject to restrictions imposed by the sender or recipient). These network devices, even though manufactured by many different companies, can communicate with one another since they use a common set of agreed-upon technical standards.

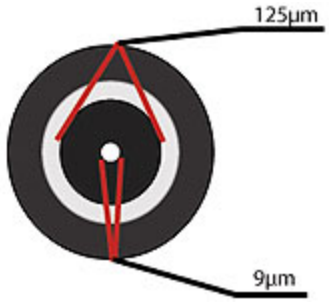
17. To communicate over the Internet an individual user must obtain a connection from an Internet Service Provider ("ISP"), either directly or indirectly through an organization such as an employer, or an Internet café (for example, a Starbucks). Typically, an ISP is a private company that provides subscribers access to the Internet for a periodic fee. Subscribers to an ISP's services can be individuals, businesses, educational institutions, government agencies, or other organizations. An ISP maintains one or more local facilities, referred to as points of presence (POPs), at which subscribers can connect with the ISP's network and thereby gain access to the rest of the Internet. Access can be provided via the twisted-pair copper cables originally installed for telephone service, coaxial cable also used to provide cable television service, fiber-optic cable, or wireless satellite signal.

18. In a residential setting the connection is ordinarily made through a device located at the subscriber's home (and often supplied by the ISP) called a router or modem. (Increasingly, however, some individual Internet users have "cut the cord" and only use services provided by cellular telephone networks.) In a business, government agency, or other large organization, the device used by an individual will be part of a local area network (LAN) operated by the organization. The local area network is then connected to the network of a local or regional ISP with which the organization has contracted. The networks of local and regional ISPs in turn connect, at locations known as regional points of presence, to the networks of still larger ISPs, the largest of which are so-called "Tier 1" telecommunication service providers such as AT&T, CenturyLink, Cogent, Verizon or their international equivalents such as NTT or Deutsche Telekom.

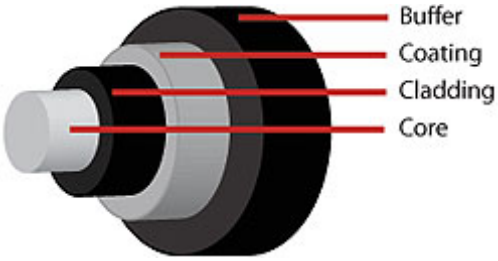
19. Tier 1 and other large carriers maintain high-capacity terrestrial fiber-optic networks, generally known as Internet "backbone" networks, which use long-haul terrestrial cables to link large metropolitan areas across entire nations or regions. (Shown below are the North American parts of Cogent's fiber-optic network.) Data travel across these fiber-optic cables in the form of optical signals, or pulses of light. Each fiber-optic cable contains between 4 and 432 glass fibers, with strand counts of around 144 common.

Cogent US domestic fiber network

Each fiber has at its core a thin, flexible strand of glass, about 9 micrometers thin, surrounded by another glass strand of 125 micrometers. (A micrometer is one-millionth (10^{-6}) of a meter. A human hair has a diameter of between 17 and 181 micrometers.) Data is transmitted by lasers, carried long distances through the insertion of optical amplifiers, and received by photo detectors.



Fiber-optic strand

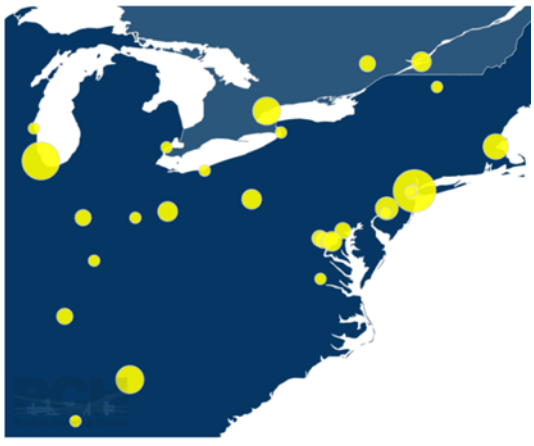


Fiber-optic cable

Buried fiber cable

20. To make possible communications between users linked to one provider's network with users linked to another's, Tier 1 providers typically interconnect (link) their networks either directly, at facilities known as private peering points, or through public Internet exchange points (IXPs). In an Internet exchange, many different telecommunication carriers can link with each other, exchanging traffic. For example, the Amsterdam Internet Exchange (AMS-IX) (shown below) connects 824 different networks, using 1,423 ports (connections), and carries about 5 terabits (5 billion bits) per second of traffic during the peak hour of the day.[1] A public directory[2] lists 905 such IXPs, differing greatly in the number of carriers that interconnect at each and the total volume of traffic carried.

AMS-IX Internet exchange (Amsterdam)[3]



Map of IXPs in eastern United States (source: PCH)

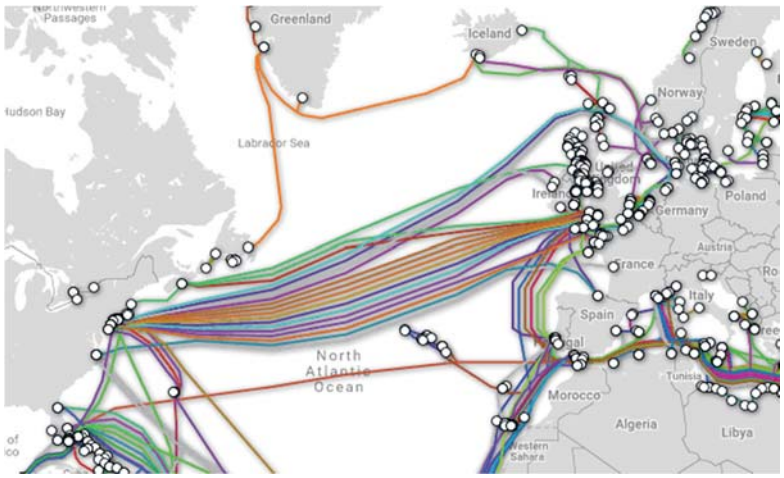
[1] https://ams-ix.net/technical/statistics

[2] https://www.pch.net/ixp/dir

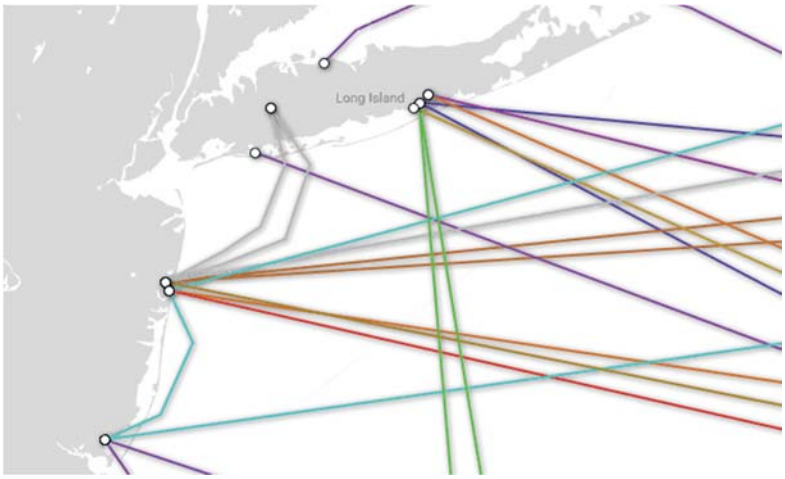
[3] https://pcmweb.nl/artikelen/internet/zo-werkt-ams-ix-alles-over-het-grootste-internetknooppunt-ter-wereld/

21. In addition to long-haul terrestrial cables, the Internet backbone also includes transoceanic cables linking North and South America with each other and with Europe, Asia, the Middle East, and Africa. These undersea cables are laid directly on the ocean floor, and make landfall at points known as cable landing stations. Technologically speaking, there is no fundamental difference between long-haul terrestrial and transoceanic links. Both types use buried fiber cable with optical amplifiers placed at regular intervals, although the hostile environment of the oceans and the difficulty of providing power to amplifiers far from shore influence design details. As an example, the recently-completed MAREA cable has landing points in Virginia Beach, Virginia and Bilbao, Spain, and is composed of eight fibers delivering a total of 160 terabits per second (160,000 billion bits per second). The fiber bundle, encased in heavy-duty metal shielding, has a diameter similar to a garden hose and is placed directly on the ocean floor, except for the shallow stretches near the landing stations, where it is buried to protect it against ship anchors and other disturbances.

22. The map below, provided by TeleGeography, illustrates some of the Internet-carrying fiber-optic cables linking the east coast of the United States to Europe.



The map enlargement below, from the same source, shows that most east coast transatlantic fibers originate from a few landing sites in New Jersey and on Long Island.



23. At each shore location, cable landing stations connect the transoceanic cable to terrestrial cable networks. An example of a cable landing station (Cape Broyle, Canada) is shown below, drawn from the manufacturer's web site.[4] It contains fiber amplifiers, management systems, and possibly Internet routers. The adjacent picture shows the inside of the same facility, showing fiber racks and ceiling cable trays. A terrestrial cable then connects the landing station to the nearest Internet exchange point (IXP), where multiple service providers then link to the terrestrial cable.

[4] http://americanmanufacturedsystemsandservices.com/products-services/products/cable-landing-stations/new-cable-landing-project.html

24. Using this infrastructure, every device connected to the Internet can communicate with every other device, no matter where located or to which providers it is connected. While the process is usually not apparent to the individual user, a communication (such as an email) being sent from one device to another across the country, or across the globe, can travel through numerous other networks en route to its destination. If the communication is traveling to a destination outside of the network of the user's ISP, it will flow onto the networks of Tier 1 or other larger providers, typically reached via an Internet exchange point, before reaching its destination via regional and local networks on the receiving end. If an international communication, it may also be carried on one or more transoceanic undersea cables, traversing cable landing stations as it exits one continent and makes landfall on the next. Such communications may traverse the networks of anywhere from one to maybe a dozen different carriers. Usually, the path is roughly similar to the shortest geographic route, but business relationships and the availability of interconnection points and transoceanic links may lead to detours, similar to how airlines may use hub airports to connect smaller or more far-flung cities.

TRANSMISSION OF COMMUNICATIONS ON THE INTERNET

25. Generally speaking, to send a communication on the Internet, the transmitting device (e.g., a personal computer, a cell phone, or the computer—a.k.a. "server"—on which a website is physically stored) first converts the communication into one or more "packets." Packets are relatively small chunks of digital information that can be transported more efficiently than transporting communications (such as entire webpages, or large documents) whole. Packets are typically between a few tens of bytes and 1,500 bytes long, where each byte, roughly speaking, can carry one text character of information. A brief discussion of network protocols and "layers" is helpful to understanding how the packets comprising a communication travel across the Internet.

26. In all communications networks, including the Internet, communicating entities need to agree on a set of technical conventions concerning how to exchange information. These conventions are generally called protocols. "A protocol defines the format and order of messages

exchanged between two or more communicating entities, as well as the actions taken on the transmission and/or receipt of a message or other event."[5] Most telecommunications protocols are defined in engineering specifications, drawn up by international bodies and revised periodically. For the Internet, protocols are primarily defined by the Internet Engineering Task Force (IETF), discussed above, in documents known for historical reasons as RFCs. Each protocol operates and serves its function within a "layer" of the communications network architecture. The concept of layering is a way of functionally sub-dividing a communications system into subsystems, or "layers," of similar functions that provide services to the layer "above" and receive services from the layer "below."

27. In the most widely used network model, the Internet protocol suite, the layers from the "bottom" to "top" of the "stack" are the physical, data link, network, transport, and application layers. For purposes here, the primary layers of interest are the physical, network, transport, and application layers. The physical layer transports electrons or photons between routers and switches, e.g., via fiber-optic or copper cable. The network layer allows two devices on the Internet to communicate with each other by making it possible for packets to travel and be exchanged across many links and networks of different providers using differing technologies. The Internet Protocol, now in two different versions, is the only widely used network-layer protocol at the moment. The transport layer ensures that the receiver can detect whether the information has arrived without error, with the Transmission Control Protocol (TCP) as the dominant protocol. TCP also retransmits any packets that may have been lost by the network and makes a sequence of packets appear as a stream of data and thus hides the packet nature of the Internet from applications using the protocol. UDP, the other transport protocol, does not provide reliability and in-order delivery. Finally, the application layer makes possible the transmission of various communications applications, such as email, or web pages, using protocols specific to each application, such as the Simple Mail Transfer Protocol (SMTP) and the

[5] J. Kurose and K. Ross, "Computer Networking: A Top-Down Approach," p. 5 (Pearson, 2017).

Internet Messaged Access Protocol (IMAP) (both for email), and the Hyper Text Transfer Protocol HTTP (for web pages). As a rough analogy to road networks, the asphalt is the physical layer, the trucks and cars offer network services, a shipping company offers a transport service, and an e-commerce company provides the application service.

28. When a communication is broken into separate packets, each packet includes (i) a "header," that is, the routing, addressing, and other technical information required by the transport protocol to facilitate the travel of the packets from their source to their intended destination, and (ii) a "payload," that is, a portion of the contents of the communication being transmitted. A rough analogy can be drawn between the transmission of packets and delivery of mail by the postal service. A business letter has a "header" containing the sender address, a date ("time stamp") and the recipient address, in addition to various processing indications, such as confidentiality markings or signatures. The letter is then placed in an envelope for delivery that displays this "header" information, but contents of the letter remain invisible to the postal service. The manner and timing of the letter's delivery is unaffected by such factors as the contents, language, or format of the letter.

29. Each layer of the communication stack uses a different header, corresponding to that layer's purpose. For our purposes here, I mainly focus on the network and transport layers. The packet headers for the network and transport layers contain three relevant pieces of address and routing information: (i) the packet's source and destination Internet Protocol (IP) addresses and (ii) protocol numbers, in the network layer header; and (iii) the source and destination ports, in the transport protocol header.

30. IP Addresses: IP addresses are unique numeric identifiers assigned to particular computers, devices, or systems connected to the Internet, and which, as the name suggests, are used by the Internet Protocol at the network layer to send data from one computer or other online device to one or more other devices, and back. IP addresses may be analogized, as in the example above, to the destination and return addresses on an envelope sent through the mail, or to telephone numbers identifying the source and destination of a call. On the telephone

network, telephone switches rely on telephone numbers, area codes, and country codes to route calls locally, within the same local exchange, and long distance. On the Internet, IP addresses fulfill a similar function.

31. Currently there are two versions of IP addresses in use. Since the 1980s the Internet has used so-called IP version 4 addresses (RFC 791, 1981), abbreviated as IPv4. There are approximately four billion such addresses. For example, the web server hosting Wikipedia (Wikimedia's largest website) has an IPv4 address written as 208.80.154.224 in the US. (It may use other addresses elsewhere.[6]) The growth of the Internet, primarily through mobile devices, has outstripped the supply of IPv4 addresses, so a new version, IP version 6 (IPv6) has been adopted that uses a greater number of characters, thus allowing for as many as 340 undecillion (10^{36}) addresses. That is sufficient to assign as many addresses as the current IPv4 provides to every star in the universe. In the United States, the Wikipedia server currently uses the IPv6 address 2620:0:861:ed1a::1. Many computers "speak" both protocols; web servers, including the Wikipedia servers, may deliver content using either Internet protocol, depending on the computer connecting to the server.

32. Each ISP or other large enterprise with a fixed presence on the Internet acquires blocks of IP addresses from the appropriate regional Internet registry affiliated with the IANA. For example, the American Registry for Internet Numbers (ARIN) allocates blocks of IP addresses to large enterprises in the United States and Canada. Columbia University has been assigned the 65,536 IP addresses from 128.59.0.0 to 128.59.255.255. Comcast uses, among many other IPv4 address blocks, the roughly eight million addresses starting at 50.128.0.0. There are public databases that record, with very high accuracy, which address blocks are used by what entities, at least at the granularity of ISPs or other large organizations that have assigned autonomous system (AS) numbers, like the Wikimedia Foundation (ASN 14907).

[6] Sites such as https://www.whatsmydns.net/ can be used to determine the IP addresses of a domain (e.g., a website) as they would appear from various geographic locations.

33. IP addresses can be assigned on a permanent or temporary basis, referred to respectively as "static" and "dynamic" addresses. Static IP addresses can be assigned directly to a "self-hosting" organization by the regional Internet registry (as in Wikimedia's case), or indirectly to businesses or other organizations that obtain Internet access via ISPs. (ISPs, after obtaining their allocations of IP address blocks from the registry, in turn assign smaller blocks of fixed addresses to their business customers.) Static IP addresses almost never change. Fixed IP addresses are necessary to run servers, as a server's IP address needs to be disseminated to client (user) computers and mobile devices that want to connect to it. For example, the IP addresses of the servers that host Amazon.com, or Wikipedia.org, must remain unchanging if online shoppers, or Wikipedia's readers and contributors, are to reach them over the Internet. As a rough analogy, static IP addresses are like business phone numbers, which typically do not change for years since they are advertised on business cards and painted on delivery vans. So that Internet users are not required to ascertain, or memorize, the IP addresses of every website they visit, a database service called the domain name service (DNS) translates the names that users type into their browsers, e.g., Wikipedia.org, into Internet addresses, e.g., 208.80.154.224.

34. While the business customers of ISPs may be allotted a fixed block of IP addresses, assigned permanently, ordinarily residential customers get exactly one "dynamic" IPv4 address at a time, assigned on a temporary basis. Dynamic IP addresses may be assigned for a day, an hour, or some other period of time, depending on the needs, resources, and business practices of a particular ISP, after which they are assigned to other customers. An ISP may even assign a particular IP address to a home customer only for the specific length of time (session) that the customer is connected to the Internet, after which the IP address may be released and assigned for temporary use by another customer. (Consumers may be assigned a block of IPv6 addresses, but again without any claim to keep that particular block.)

35. Ports: IP addresses alone are not sufficient to operate networks having multiple functions. For example, the same server may host a web service, an email service and a voice-over-IP (Internet telephony, a.k.a. VoIP) service. The operating system on the server, such as

Windows or Linux, uses *port numbers*, carried in the transport layer protocol (typically TCP or UDP), and included in the header of each communication packet, to distinguish packets destined for the web service from those meant for the email or VoIP services. Likewise, on the user's end, a client computer (a home or office computer, or mobile phone) may run multiple applications for various online activities, such as web-browsing, sending and receiving email, or voice communications using VoIP technology. The user's device also uses port numbers contained in packet headers to ensure, for example, that pages downloaded from a website are routed to the user's browser, not his or her email application, and vice versa.

36. While IP addresses used to route a communication to a particular destination device can be analogized to the street address on a letter, or to a telephone number, port numbers are roughly analogous to the apartment numbers at a multi-unit dwelling, or individual extensions to a business telephone number. Port numbers for common applications like web-browsing and email, each with its own application-layer protocol, are maintained in a common industry registry maintained by the IANA. Some common port number assignments are in the table below; they are generally numbers between 1 and 49,151.

Port number	Protocol	Application
20	ftp	File transfer
22	ssh	Remote login
25	SMTP	Mail delivery between servers
53	DNS	Domain name system (host name lookup)
80	HTTP	Web pages, unencrypted
123	NTP	Network time (clock) synchronization
143	IMAP	Remote email message access
443	HTTPS	Encrypted web pages, using SSL/TLS

587	SMTP	Email submission protocol, from client to server
993	IMAP	Email access, encrypted using TLS
5060	SIP	VoIP session setup

37. It is possible to run network applications on non-standard ports, but then users on both ends of the communication have to be aware that this is being done. For example, http://portquiz.net:8080/ is a website that uses port 8080, but needs to indicate that fact by including the port number in the web address (URL). Some applications, such as the media (voice or video) components of voice-over-IP, do not have fixed port numbers; rather, devices on each end of the conversation agree on suitable port numbers on a call-by-call basis.

38. Protocol Numbers: Protocols associated with various layers of the network architecture are also assigned numbers maintained in a registry by the IANA. Protocol numbers are also included in packet headers and used by receiving devices to determine the appropriate protocols to apply for interpreting and acting on each packet upon arrival.

39. Once a communication has been broken into constituent packets by the transmitting device, the job of ensuring that the packets travel an appropriate path across the Internet from their source to their destination IP address is performed by devices known as routers and switches. Routers and switches are specialized computers, located at strategic network points, that take on a similar role for the Internet as switches on the telephone network. That is, their basic function is to determine where on the Internet to send packets next. Packets constituting a single communication can travel through several to as many as dozens of routers and switches to reach their destination. Typically, so-called carrier- or enterprise-grade routers are located at ISP points of presence (POPs), peering stations, or Internet exchanges, routing packets from one network to another. A large router commonly found in such Internet exchanges is shown below. Carrier- or enterprise-grade switches are typically located at points of presence where different legs of the same carrier backbone network interconnect, and forward packets from one leg of the network to another.

Juniper router ((c) Juniper Networks)

40. To perform its function, each router or switch along a packet's path "decodes" the incoming light pulses from the connected fiber-optic cable and reconstitutes the individual packets for processing. The router or switch then scans each packet's header information, including its destination IP address, and matches the address against an internal routing table. The routing table contains rules (updated by a routing protocol) determining the direction in which packets with addresses falling in particular IP ranges should be forwarded. This exercise may leave the router or switch with a choice of anywhere between three and hundreds of possible next-leg destinations for the packet. The routing protocol can also be used to convey performance-based rules for determining which of the available paths to choose. This allows the router or switch to find a connection with good performance, avoid congested connections, detour packets around failed network links, and use newly available connections, somewhat similar to the manner in which Google Maps updates the fastest route to take between a user's starting point and his/her destination. The largest routers and switches, those used to handle exchanges of communications data at major intersections on the Internet, handle millions of data packets every second.

41. While, in theory, each packet in a single communication could take a different path across the Internet, in practice packets traveling between two points on the Internet generally follow the same path for long distances, just like most motorists traveling between New York City and Washington, D.C., take Interstate 95, following different possible paths (like different county

roads, or neighborhood streets) only when nearing their destinations, or to avoid traffic jams. In particular, since transoceanic connections are only added and removed infrequently, and since most carriers only have a few links that they use, any traffic between international destinations is likely to keep using the same fiber links for months, if not years, except for routing around any outages. Generally, traffic takes the shortest route, subject to business arrangements between carriers. For example, packets comprising an email sent from New York to Amsterdam will traverse the Atlantic Ocean via undersea cable to a landing site in northern Europe, rather than take a circuitous route via the Pacific Ocean, or even a southern route across the Atlantic via Africa.

42. To protect the privacy and integrity of information, users sending data across the Internet may choose to encrypt their traffic, i.e., convert the data into code by a mathematical transformation, so that it can only be read by parties who have the encryption key. Generally, modern encryption techniques are considered to be unbreakable by any third party that does not have access to the key, even if the encryption mechanism is known. The most common encryption mechanism is the Transport Layer Security (TLS) protocol, which operates at the transport layer, one below the web HTTP protocol. The combined use of TLS and HTTP is commonly referred to as HTTPS, even though it is not a single protocol and TLS can also be used for other applications. Use of the encrypted HTTPS protocol is designed to ensure that information sent to or from a web site can only be read by the user's web browser and the host web server, but not third parties, including entities capable of copying packets en route between the browser and the web server. HTTPS offers the exact same functionality of retrieving web pages, but ensures that the web browser connects to the correct web server, and that no third party can read the content of the communications. Despite its relation to HTTP, HTTP-over-TLS (HTTPS) has been assigned a different port, port 443 (the unencrypted HTTP protocol is assigned port 80), allowing web browsers and web servers to distinguish encrypted from unencrypted information by the port number.

43. Increasingly, most popular websites, including those of the Wikimedia Foundation, use HTTPS or at least offer their content via both HTTP or HTTPS. In fact, given the commonality of encryption today, most entities with an Internet presence offer an encrypted version of their content, and the temporary use of unencrypted content to, for example, support legacy applications that have not yet made the transition, is increasingly rare.

44. Once the packets making up a communication arrive at the receiving computer or smartphone, the operating system of the receiver reassembles the packets into the original communication, such as a web page or email, even if the network between the sender and receiver discards, corrupts or reorders some of the packets. As noted earlier, TCP, a transport layer protocol, performs this service, by retransmitting missing or corrupted packets.

PUBLICLY AVAILABLE INFORMATION ABOUT NSA "UPSTREAM" COLLECTION

45. NSA "Upstream" collection of communications is described, in general terms, in a number of official public reports issued by the Government, albeit not all of them authored or released by the NSA. Because such reports are relied on by Wikimedia in its Amended Complaint to inform its view of how Upstream collection might work, I rely on them as well.

46. According to these reports, once the necessary approvals are obtained from the Foreign Intelligence Surveillance Court, NSA analysts identify non-U.S. persons located outside the United States who are reasonably believed to possess or receive, or are likely to communicate, designated foreign-intelligence information. NSA Civil Liberties and Privacy Office Report, NSA's Implementation of FISA Section 702 at 4 (Apr. 16, 2014) ("NSA Civil Liberties Report), available at https://www.nsa.gov/Portals/70/documents/about/civil-liberties/reports/nsa_report_on_section_702_program.pdf. Once the NSA has designated such persons as targets, it then tries to identify specific means by which the targets communicate, such as email addresses or telephone numbers, which are referred to as "selectors." See NSA Civil Liberties Report at 4; Privacy & Civil Liberties Oversight Board Report on the Surveillance Program Operated Pursuant to Section 702 of the FISA at 32-33, 36 ("PCLOB Section 702 Report") available at https://www.pclob.gov/library/702-Report.pdf. A telecommunications service

provider may then be compelled to provide the Government all information or assistance necessary to acquire communications associated with the selector, a process referred to as "tasking." NSA Civil Liberties Report at 4-5; PCLOB Section 702 Report at 32-33.

47. Upstream collection is one of the methods through which the NSA receives information concerning tasked selectors. Upstream collection occurs as communications transit the Internet backbone within the United States. PCLOB Section 702 Report at 36-37. Under Upstream collection, tasked selectors are sent to a U.S. electronic-communications-service provider to acquire communications that are transiting the Internet backbone. PCLOB Section 702 Report 36-37. Internet communications are first filtered to eliminate potential domestic communications, and are then scanned to capture only communications containing the tasked selector. PCLOB Section 702 Report at 37. Unless communications pass both these screens, they are not ingested into NSA databases. PCLOB Section 702 Report at 37.

WIKIMEDIA'S CONTENTIONS

48. Wikimedia alleges in its First Amended Complaint that "[t]he NSA conducts Upstream surveillance by connecting surveillance devices to multiple major internet cables, switches, and routers on the internet backbone inside the United States," for the purpose of "enabl[ing] the comprehensive monitoring of international internet traffic." (Amended Complaint ¶¶ 47, 48). Wikimedia envisions Upstream surveillance as encompassing four processes, some implemented by telecommunications service providers at the NSA's direction:

- **Copying:** the use of surveillance devices, installed at key access points along the internet backbone, to make a copy of substantially all international text-based communications, and many domestic ones, flowing across certain high-capacity cables, switches, and routers.
- **Filtering:** the attempted exclusion of wholly domestic communications from the copied stream of internet data, perhaps using IP filters, while preserving the international communications.
- **Content review:** review of the full content of copied communications for the NSA's search terms, called selectors, including email addresses, phone numbers, IP addresses, and other identifiers believed by the NSA to be associated with foreign intelligence targets.

- **Retention and Use:** the retention of communications containing selectors associated with NSA targets for querying and review by NSA analysts, and sharing of the results with the Federal Bureau of Investigation.

(Amended Complaint ¶ 49)

49. I reiterate that I have not been given access to classified or other non-public information about Upstream surveillance, and so have no knowledge or information concerning the accuracy of Wikimedia's description of the Upstream collection process.

50. Wikimedia maintains that it is "virtually certain" that the NSA "has intercepted, copied, and reviewed" at least some of its communications in the course of conducting Upstream surveillance (Amended Complaint ¶ 60), based on several assumptions. First, Wikimedia asserts that given "the geographic distribution of [its] contacts and communications across the globe," with "individuals in virtually every country on earth," its communications "almost certainly traverse every international backbone link connecting the United States with the rest of the world." (Amended Complaint ¶¶ 60, 61) Second, and critically for purposes of this declaration, Wikimedia posits that "as a technical matter" the NSA "must be" copying and reviewing all international text-based communications transiting any link it is monitoring, in order to "reliably" obtain communications to or from its targets. (Amended Complaint ¶ 62) This is so, according to Wikimedia, because (i) the NSA cannot know beforehand which communications will contain selectors associated with its targets, and so must copy and review them all in order to identify those of interest, and (ii) in order to review the contents of a communication for the presence of a targeted selector, the NSA must first copy and reassemble all the packets making up that communication, requiring that it copy all packets traversing a given backbone link in order to reassemble and review communications in the manner Wikimedia describes. (Amended Complaint ¶¶ 62, 63)

51. On these premises, Wikimedia concludes that "even if the NSA conducts Upstream surveillance on only a single internet backbone link, it must be intercepting, copying, and reviewing at least those communications of [Wikimedia] traversing that link." (Amended Complaint ¶¶ 64) For the reasons I discuss in the following two sections, Wikimedia's conclusion

is incorrect. Even assuming, hypothetically, that the NSA conducts Upstream collection in the manner Wikimedia posits, by connecting collection equipment to routers and switches at links on the Internet backbone, there are a number of methods by which the NSA could be conducting Upstream surveillance without intercepting (much less copying or reviewing) all communications transiting any Internet backbone link it (hypothetically) monitors. Using these methods, the NSA could conduct Upstream surveillance without intercepting, copying, reviewing, or otherwise interacting with communications of Wikimedia. This would be true regardless of where on the Internet, or at how many locations, the NSA conducts Upstream collection.

WHETHER THE NSA "MUST BE" INTERCEPTING, COPYING, AND REVIEWING ALL COMMUNICATIONS THAT TRAVERSE A GIVEN INTERNET BACKBONE LINK

52. Wikimedia bases its belief that the NSA, in the course of Upstream collection, "must be" intercepting, copying, reviewing, or otherwise interacting with Wikimedia's online communications on the premises (i) that the NSA must be conducting Upstream surveillance at one or more Internet backbone links, such as peering points, Internet exchanges, points of presence, or cable landing stations, and (ii) that the NSA, at any given link where Upstream collection is conducted, must, as a matter of technical necessity, be intercepting, copying, and reviewing all communications crossing that link (including, therefore, Wikimedia's). I have no information concerning the actual number or location(s) of the site(s) at which the NSA conducts Upstream surveillance, so for purposes of my analysis I accept the first of these premises as given, that Upstream surveillance must be conducted at one or more links constituting the Internet backbone.

53. The second premise, however, is incorrect. As I explain below, there are a number of technically feasible, readily implemented means of conducting Upstream-type surveillance that would not require interception, copying, reviewing, or otherwise interacting with all communications that traverse any Internet backbone link the NSA allegedly monitors. I do not mean to suggest that the NSA is, in fact, conducting its surveillance by any of these means, or that these are the only possible methods by which the NSA could be conducting Upstream

surveillance. As I have stated elsewhere in this declaration, I have no knowledge or information concerning how Upstream surveillance is actually conducted. What I am saying is that, regardless of the number or types of locations on the Internet backbone at which the NSA might be conducting Upstream surveillance, there are at least several practical means for conducting that surveillance, in a manner akin to that posited by Wikimedia, that would not involve intercepting, copying, reviewing, or otherwise interacting with, all communications transiting the links the NSA allegedly monitors, thus disproving Wikimedia's hypothesis that such interception, copying, review, or other interaction with all communications "must be" occurring.

54. There are at least two well-known approaches to obtaining copies of Internet communications at locations other than the sources or destinations of the communications (or an ISP's server), which is to say, while the communications are still in transit. Locations where either of these approaches could be implemented include, but are not necessarily limited to, peering points, Internet exchanges, cable landing stations, and Internet points of presence.

55. Under the first approach, an entity desiring to obtain copies of communications for purposes of surveillance (or otherwise) could intercept the pulses of light carried on an optical fiber through the use of a device called a fiber-optic splitter (also referred to as an optical splitter). As its name suggests, a splitter, when attached to an optical fiber, "splits" the light signals on the fiber, making an identical copy of the communications stream. Through the use of one or more splitters, an exact duplicate of the communications stream flowing over each fiber-optic cable at an Internet exchange point, cable landing station, or other location could be made. The original communications could continue to travel uninterrupted to their intended destinations on the Internet, while copies of all the communications in each stream could be diverted elsewhere for processing to identify communications of interest.

56. Fiber-optic splitters are passive devices that are incapable of copying selectively, that is, they are incapable of copying only certain communications, but not others, according to specified criteria. Hence, the use of fiber-optic splitters to obtain copies of online

communications for surveillance purposes would entail, as alleged by Wikimedia, the copying of all communications flowing across a given fiber-optic link. (Amended Complaint ¶¶ 49, 62)

57. In contrast, the second approach to obtaining copies of Internet communications while in transit would allow for selectively copying only those communications that are deemed more likely to include communications of interest, without copying or otherwise handling those that are not. This approach would be desirable from the perspective of reducing the volume of communications that must be processed (electronically scanned) to identify the communications of interest, which would in turn reduce the associated time and expense. This selective copying of communications can be accomplished through the use of intelligent devices such as routers and switches (specialized computers, as discussed above), operated by carriers, to "mirror" selected communications carried in a given communications stream.

58. "Mirroring" is the technical term for a process which may be described as follows. As discussed in paragraph 40, above, when the light pulses on a fiber-optic cable enter a router, or a switch, the device "decodes" the stream into individual packets, and examines the address and routing information contained in the header of each packet, to determine where on the Internet each packet should be forwarded next. In the course of this process, the router, or the switch, can also "mirror" some or all of the traffic by making copies of selected packets, and diverting the designated copies off-network for separate processing. Almost all carrier-grade routers and switches, of the kind found at Internet exchanges and regional points of presence, are capable of traffic mirroring, as this functionality is required in order to conduct routine operational monitoring of a carrier's network. For example, traffic mirroring is used as a means of detecting denial-of-service attacks (intentionally flooding a device or network with traffic to force a shutdown and render it inaccessible to its intended users), or of ensuring that a carrier's traffic-routing policies are being properly implemented. Traffic mirroring does not interfere with the delivery of packets and is invisible to both the source and destination of the traffic.

59. Cisco Systems, the largest vendor of carrier-grade routers (based on market-share data from Dell'Oro and IDC[7]), describes the traffic-mirroring process as follows:

> "Traffic mirroring, which is sometimes called port mirroring, or Switched Port Analyzer (SPAN) … enables you to monitor Layer 3 network traffic passing in, or out of, a set of Ethernet interfaces. You can then pass this traffic to a network analyzer for analysis. Traffic mirroring copies traffic from one or more Layer 3 interfaces or sub-interfaces and sends the copied traffic to one or more destinations for analysis by a network analyzer or other monitoring device. Traffic mirroring does not affect the switching of traffic on the source interfaces or sub-interfaces, and allows the mirrored traffic to be sent to a destination next-hop address."[8]

60. Traffic mirroring can be employed to provide a collecting entity with access to select copies of communications transiting a particular Internet link, using fine-grained controls known as access control lists (ACLs). Routers are programmed using ACLs to determine whether packets are forwarded or blocked at a given router interface, that is, a given link between the router and another device.[9] Each of a router's interfaces has an associated ACL with criteria defining which types of packets may pass through the interface, and which not. The criteria used include a packet's source or destination IP address, the port number, protocol numbers, or other information contained in a packet header. The router examines the header information of each packet it processes, and compares it to the criteria established by the ACLs corresponding to each interface, to determine which interfaces the packet may or may not pass through. The router then allows separate copies of the packet to pass, in other words, to be mirrored, through each of the interfaces whose criteria it satisfies, as specified in the associated ACL.

61. Carrier-grade switches, too, can be programmed with access control lists, and, in the same fashion as a router, a switch uses the criteria in the ACLs associated with each of its

[7] https://www.telecomlead.com/telecom-statistics/cisco-leads-service-provider-router-and-carrier-ethernet-switch-market-84577

[8] Cisco, "Configuring Traffic Mirroring on the Cisco IOS XR Software," Manual; available at https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r5-1/interfaces/configuration/guide/hc51xcrsbook/hc51span.pdf.

[9] RFC 4949 (2007) defines ACL: "A mechanism that implements access control for a system resource by enumerating the system entities that are permitted to access the resource and stating, either implicitly or explicitly, the access modes granted to each entity."

interfaces to determine which packets processed by the switch can pass (be mirrored) through each interface.

62. Carriers routinely use access control lists for a variety of reasons, one of the most important being network security. ACLs prevent packets coming from other carriers' or providers' networks, or from less secure areas of a carrier's own network, from entering more sensitive areas of the carrier's network. The use of access control lists to control the flow of network traffic is sometimes referred to as filtering. Publicly available documentation from Cisco explains the filtering capabilities of its carrier-grade routers using access control lists.[10] The skills required to configure ACLs and load them into a router are part of the repertoire of any trained network technician.

63. Cisco produces two commonly used models of router, the Cisco CRS and ASR, that support traffic mirroring.[11] The figure below, drawn from related Cisco documentation[12] shows a simplified schematic representation of a network topology wherein the network analyzer (i.e., the collecting entity's equipment) receives some or all of the packets sent between transmitting device A and receiving device B. The access control lists (ACLs) supported by Cisco devices can restrict or allow packets' passage based on either source or destination characteristics, including the interface (*e.g.*, a particular fiber), Internet (IP) address, the Internet protocol version (IPv4 or IPv6), the next-layer protocol (*e.g.*, IPsec or TCP), or the port number.[13] The number of ACL entries varies depending on the hardware. For example, the Cisco ASR 9000 router supports up to 4,095 unique access control lists. The practical limits of the number of white list or black list

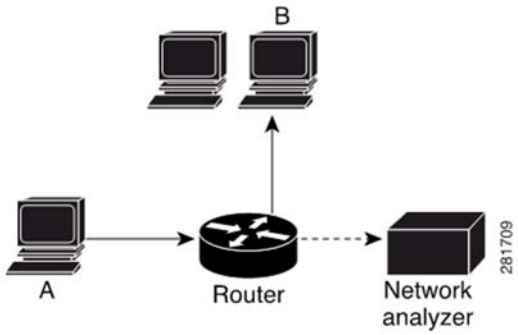
[10] https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r4-0/addr_serv/command/reference/ir40asrbook_chapter1.html is one example of this capability.

[11] https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r5-1/interfaces/configuration/guide/hc51xcrsbook/hc51span.pdf and https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r5-1/interfaces/configuration/guide/hc51xasr9kbook/hc51span.html#96505

[12] https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r4-1/interfaces/configuration/guide/hc41asr9kbook/hc41span.pdf

[13] https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r4-0/addr_serv/command/reference/ir40asrbook_chapter1.html#wp49507452

entries depends on the router model and may vary. Other router vendors support similar functionality.



64. Traffic mirroring through the use of access control lists could likewise be used in a surveillance context to make only certain packets available for inspection by the collecting entity at any given link on the Internet where surveillance may be conducted. There are several ways in which this could be accomplished. Initially, it would be necessary to establish a link between the router, or switch, directing traffic at that location, and the separate set of equipment used by the collecting entity (wherever situated) to electronically scan the packets to which it is given access for communications of interest.

65. Once the link is established, traffic passing through the carrier's router, or switch, to the collector's equipment could be filtered by various "whitelisting" or "blacklisting" techniques, defined below, that involve configuration of an access control list that allows only packets meeting the ACL's criteria to be copied and passed through the interface to the collector's equipment. For example, if the collecting entity possesses information that communications of interest to it are associated with a particular IP address, or set of IP addresses, then it could request that the carrier provide it only with packets whose source or destination IP addresses match the IP addresses of interest. (I assume for purposes of this discussion that the "tasking" described earlier can go beyond simply enumerating targeted email addresses or phone numbers to the carrier, i.e., include limitations on the protocols, sources and destinations of Internet traffic to be made available for NSA examination.) The carrier, in turn, could configure the ACL of the appropriate interface with a "whitelist" of the specified IP addresses. As a result,

when the router (or switch, as the case may be) examines the header information of each packet it processes, it would, as usual, forward a copy of the packet (as determined by its routing tables) toward the packet's intended destination, possibly create and forward additional copies of the packet through other interfaces, depending on the routine policies and practices of the carrier, and if, but only if, the packet header contains a source or destination IP address on the designated whitelist, create an additional copy of the packet and forward it through the interface with the collector's equipment to the collector's possession and control.

66. Packets not meeting the whitelist criteria would not be copied for, or made available to, the collector's equipment for reassembly, review, retention, or any other purpose, and would not be handled or processed in any way other than would ordinarily occur under the carrier's routine practices.

67. Blacklisting, as the name suggests, is the converse of whitelisting. Tipton and Krause define them as follows in a more general information security context: "Blacklisting consists of banning a list of resources from access. … Whitelisting is listing entities that are granted a set of privileges (access, services, validity, etc.) within an environment. A whitelist is solely used to define what is allowed to be executed, whereas anything that is not included in the whitelist cannot be executed."[14] Blacklisting involves the configuration of an access control list that allows all packets to pass through the interface with the collector's equipment except those meeting the ACL's criteria. For example, the collecting entity might conclude that communications traffic to and from certain IP addresses, perhaps by virtue of the geographic locations or the organizations they are associated with, are of little interest for the collector's purposes, and that these communications burden the processing capacity of its equipment without yielding information of significant value. In that situation, the collector may advise the carrier that it does not wish to receive traffic to and from these "low-yield" IP addresses. In that case, the carrier could configure the ACL corresponding to the interface with the collector's

[14] Harold Tipton and Micki Krause, "Information Security Management Handbook," CRC, 2007.

equipment with a "blacklist" of the specified IP addresses. Once so programmed, the router, or switch, would as usual examine the header of each packet it processes, forward each packet toward its destination on the Internet, create and forward copies of each packet through various interfaces as dictated by the carrier's business practices, and create an additional copy of each packet, and forward it through the interface with the collector's equipment to the collector's possession and control, *except* for those packets with source or destination IP addresses on the designated blacklist.

68. If on examination a packet is found to contain a source or destination IP address on the blacklist, an additional copy of that packet is not created or forwarded through the interface to the control of the collecting entity, and would not be handled or processed in any way other than would ordinarily occur under the carrier's routine practices.

69. Whitelisting and blacklisting techniques can also be used to limit mirroring to particular sources of traffic. For example, if a router at an exchange, landing station, or point of presence is linked to multiple fiber-optic cables used respectively by different carriers, or linked to particular countries, mirroring can be restricted to traffic only from certain carriers' networks, or certain global regions.

70. In addition, whitelisting and blacklisting can be used to mirror only particular kinds of communications based on their protocols. As discussed above, communications of different types, having different protocols, are assigned different port numbers to ensure that user communications, or requests for information, are directed to the appropriate service hosted on the recipient server, and that the response to the user is directed to the appropriate application on the user's computer, cellphone, or other device. The access control list associated with the interface between a router or switch and a collecting entity's equipment can also be configured to whitelist or blacklist distinct types of communications based on their assigned port numbers. Suppose, for example, that the collecting entity is interested only in examining email. Email communications use the SMTP and IMAP protocols, the default ports for which are port 25 and port 143, respectively. If advised by the collecting entity that it only wishes to examine email

communications, the carrier could configure the ACL corresponding to the router interface with the collector's equipment to create additional copies of packets, and forward them to the collector's control, only if the port number contained in the packets' headers is port 25 or 143.

71. On the other hand, the collecting entity may determine that certain types of communications yield little information of value, and simply burden the capacities of its processing equipment. In that event, the collecting entity may inform the carrier that it does not wish to receive communications of that type. The carrier could then configure the appropriate ACL so that packets containing port numbers corresponding to those undesired types of communications are not copied and passed through the interface to the collecting entity's control. For example, as discussed above, the encrypted HTTPS protocol, used to communicate with sites on the World Wide Web, provides a high degree of assurance that communications sent to or from a website can only be read by the user's web browser and the host web server, but not third parties who intercept them in transit. A collecting entity, if it lacks the capability of decrypting HTTPS communications, and therefore can glean no useful information from them, might advise an assisting carrier that it does not wish access to such communications. Because HTTPS communications are assigned port number 443, the carrier could simply configure the access control list for the interface with the collecting entity's equipment so that no packets containing port number 443 are copied and passed to the collecting entity's possession and control.

72. Wikimedia, in fact, posits a highly similar type of scenario in its Amended Complaint. Wikimedia states:

> By some estimates . . . two-thirds of internet traffic consists of video traffic. The NSA could readily configure its surveillance equipment to ignore that traffic, or at least the significant portions of it (e.g., Netflix traffic) that are almost certainly of no interest. Because of the substantial efficiency gains to be had, it is extremely likely that the government engages in this kind of filtering . . . .

Amended Complaint ¶ 59. To achieve the result hypothesized by Wikimedia, the carrier at any Internet link where the NSA might theoretically be conducting Upstream surveillance could "readily," as Wikimedia says, configure the access control list associated with the interface

between the carrier's router or switch and the NSA's surveillance equipment to block transmission of any packets whose source IP addresses correspond to the streaming video services whose traffic the NSA did not wish to have access to.

73. As mentioned above, Wikimedia gives two specific reasons why it believes the NSA nevertheless "must be" copying all the international text-based communications that travel across any given Internet link where it conducts Upstream surveillance. I address both here. First, Wikimedia maintains that because the NSA cannot know beforehand which international, text-based communications traversing a link will contain selectors associated with its targets, it must copy and review them all in order to "reliably" identify those of interest. (Amended Complaint ¶ 62) The foregoing discussion of traffic mirroring demonstrates that this is not necessarily the case. If a collecting entity, by whatever means, were to ascertain to an acceptable degree of confidence that the communications of interest to it are associated with particular IP addresses, then by whitelisting packets containing those IP addresses in their headers, it can reliably obtain the packets of all communications to and from those IP addresses crossing that link, without obtaining access to any other communications crossing that link. Conversely, if the collecting entity ascertained to an acceptable degree of confidence that communications to and from certain IP addresses do not include communications of interest to it, then by blacklisting communications to and from those "low-interest" IP addresses, it could reliably obtain all communications of interest that are crossing that link without obtaining access to any of the blacklisted communications. And in either scenario, the packets not accessed would undergo no handling or processing other than would ordinarily occur under the carrier's routine practices.

74. The question remains, of course, how confident would a collecting entity have to be that it could "reliably" acquire its targets' communications using these more selective approaches, based on IP addresses (or port or protocol numbers), before it would deem them acceptable. Speaking as someone who has studied the economics as well as the technology underlying large-scale network engineering, I would say that the answer to that question

depends on the collector's objectives, capabilities, resources, and competing organizational priorities. So far as this case is concerned, these are all matters known only to the NSA.

75. Second, Wikimedia maintains that the NSA cannot "reliably" obtain its targets' communications without copying and reviewing all international text-based communications traveling across a link because, according to Wikimedia, to review a communication for the presence of a targeted selector, the NSA must first copy and reassemble all the packets making up that communication. (Amended Complaint ¶ 63) This reasoning is flawed.

76. It is not the case that all the packets on a communication link must be collected before the communication of interest can be reassembled. Each set of communication relationships and protocols is independent. For example, an email communication between two parties does not depend on a web transfer, either between those two parties or any other party, and reassembling the web communication is neither necessary nor helpful to obtain or analyze the email communications. Thus, it is sufficient to reassemble only the email-related packets, identifiable by protocol number and port, if email is of interest. All of the packets in a communication to or from an individual target will have a common destination or source IP address, respectively. If the target can be identified by IP address or range of addresses, and if the collecting entity obtains access to all packets crossing the link that contain that address (or an address falling in that range), it will have all the packets making up that communication, and can reconstruct it. Through traffic mirroring, this objective can readily be achieved either by whitelisting packets containing IP addresses associated with communications of interest, or blacklisting communications to and from IP addresses that are likely of no interest. In either case, it would not be necessary, as a technical matter, to copy all packets crossing the link in order to "reliably" reassemble and identify communications of interest, so long as the collecting entity itself were sufficiently confident in its ability to identify the IP addresses of high-interest communications, or communications (and their IP addresses) that are of low interest.

WHETHER THE NSA "MUST BE" INTERCEPTING, COPYING, AND REVIEWING WIKIMEDIA'S ONLINE COMMUNICATIONS

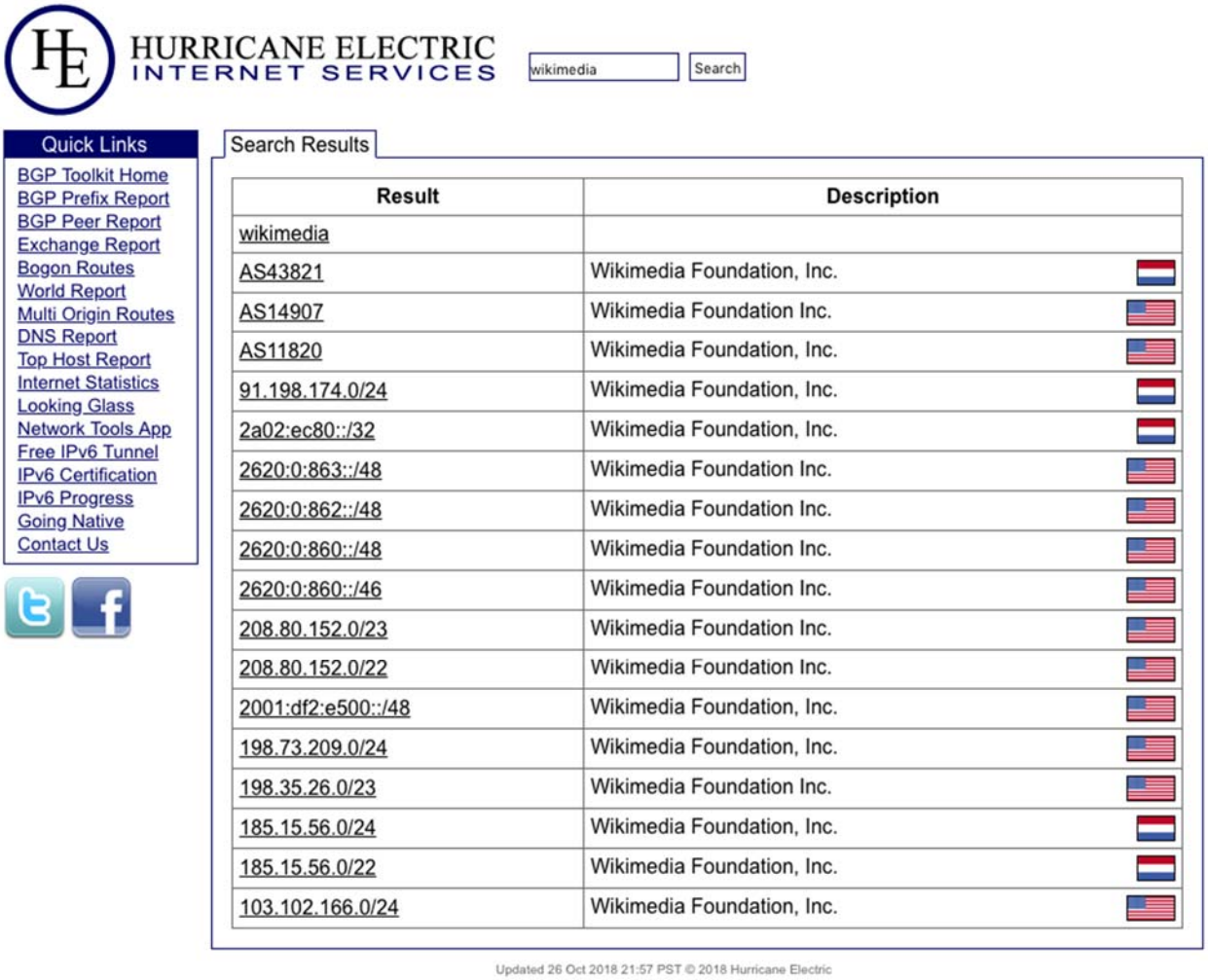
77. In this section I explain how the NSA, through the use of traffic-mirroring techniques such as those discussed in the preceding section, could conduct Upstream-type surveillance in a manner similar to that posited by Wikimedia without intercepting, copying, reviewing, or otherwise interacting with communications of Wikimedia. I emphasize, again, that I do not mean to suggest that the NSA in fact employs any of these techniques in conducting Upstream collection, only that they are technically feasible, readily implemented means by which it could do so without intercepting, copying, reviewing, or otherwise interacting with Wikimedia's communications. I am advised by Justice Department counsel that Wikimedia has identified three categories of its communications that it believes are subjected to Upstream collection processes: (1) communications with and among its "community members," that is to say, individuals who read or contribute to its websites; (2) its server log communications; and (3) communications to and from its staff. I discuss each category below in turn.

78. Category 1 (communications with and among "community members"): In a chart entitled "Technical Statistics for 2017 to 2018 Responsive to ODNI Interrogatory No. 19," Wikimedia describes the first category of its allegedly intercepted communications as "Wikimedia communications with its community members, who read and contribute to Wikimedia's Projects and webpages, and who use the Projects and webpages to interact with each other." It specifies three types of communications as falling within this first category, HTTP and HTTPS requests from foreign users to Wikimedia servers in the United States (presumably requests to view or download content from Wikimedia websites); HTTP and HTTPS requests from users in the United States to foreign Wikimedia servers (presumably the same), and SMTP communications from foreign users to Wikimedia servers in the United States (presumably email). In brief, then, Category 1 communications consist of traffic using the HTTPS protocol (i.e., encrypted web traffic), the HTTP protocol (unencrypted web traffic) and the SMTP protocol (email traffic), all destined to a limited number of IP addresses used by Wikimedia, that are also listed in the chart.

79. To my knowledge, the Government has publicly acknowledged that the NSA uses email addresses and telephone numbers as "selectors" to identify communications involving its Upstream targets, but has not publicly confirmed whether or not it uses any other kind of identifier for that purpose. It is therefore unknown (at least publicly) what types of communications other than email or telephone calls, if any, that the NSA acquires via Upstream collection. If, hypothetically, the NSA does not collect web communications, whether due to their volume, because they may be of insufficient interest, or both, then it would stand to reason that the NSA, at any link where Upstream surveillance may be conducted, might not seek access to traffic using either of the current web protocols, HTTP and HTTPS. (If the NSA does not possess the capability to decipher encrypted HTTPS communications—whether it does or does not I do not know—then that is an additional reason it might regard such unreadable communications to be of low interest.) Using a blacklisting approach such as I describe above, the assisting carrier could block any HTTP and HTTPS traffic transiting that link (*i.e.*, packets with port numbers 80 and 443, respectively) from being forwarded to the NSA's collection equipment. Under such a scenario, none of Wikimedia's HTTP or HTTPS communications crossing that link would be intercepted or copied (other than for the carrier's own purposes, if any) and would not be made available to the NSA. If the NSA, for whatever reason, were not interested in collecting web communications, including Wikimedia's, there is no technical reason why it would nevertheless be compelled to intercept, copy, or review them, as Wikimedia suggests.

80. Even if HTTP and HTTPS communications are not excluded, as a general matter, from those the NSA obtains access to for Upstream purposes, Wikimedia's web communications could still be subject to exclusion from the communications provided to the NSA at any given link, through whitelisting or blacklisting. As reflected in Wikimedia's technical statistics chart, Wikimedia has been allocated a number of static (permanent) IP addresses, as is essential for users around the world to access and contribute to its public websites. For the same reason, these addresses are publicly disseminated, and are available from online directories that track organizations' IP addresses according to their assigned AS (autonomous system) numbers.

(Shown below is an example from Hurricane Electric, a well-known Internet backbone carrier.) Additionally, for global routing of international traffic, each router or switch located at a link on a major carrier's network contains an accessible registry, also organized by AS number, of the IP addresses that can be reached via that link. Anyone knowledgeable in the realm of network traffic management would have the skill needed to access these registries and compile a list of all IP addresses associated with any organization, such as Wikimedia, that has been assigned its own AS number. That list could be used, in turn, to exclude communications associated with such an organization, including Wikimedia.


HURRICANE ELECTRIC INTERNET SERVICES

wikimedia Search

Quick Links

BGP Toolkit Home
BGP Prefix Report
BGP Peer Report
Exchange Report
Bogon Routes
World Report
Multi Origin Routes
DNS Report
Top Host Report
Internet Statistics
Looking Glass
Network Tools App
Free IPv6 Tunnel
IPv6 Certification
IPv6 Progress
Going Native
Contact Us

Search Results

Result	Description
wikimedia	
AS43821	Wikimedia Foundation, Inc.
AS14907	Wikimedia Foundation Inc.
AS11820	Wikimedia Foundation, Inc.
91.198.174.0/24	Wikimedia Foundation, Inc.
2a02:ec80::/32	Wikimedia Foundation, Inc.
2620:0:863::/48	Wikimedia Foundation Inc.
2620:0:862::/48	Wikimedia Foundation Inc.
2620:0:860::/48	Wikimedia Foundation Inc.
2620:0:860::/46	Wikimedia Foundation Inc.
208.80.152.0/23	Wikimedia Foundation Inc.
208.80.152.0/22	Wikimedia Foundation Inc.
2001:df2:e500::/48	Wikimedia Foundation, Inc.
198.73.209.0/24	Wikimedia Foundation, Inc.
198.35.26.0/23	Wikimedia Foundation Inc.
185.15.56.0/24	Wikimedia Foundation, Inc.
185.15.56.0/22	Wikimedia Foundation, Inc.
103.102.166.0/24	Wikimedia Foundation, Inc.

Updated 26 Oct 2018 21:57 PST © 2018 Hurricane Electric

81. Therefore if, at a given link, the NSA was being given access only to communications to or from specified IP addresses (whitelisting), and Wikimedia's addresses were

not among them, then the NSA would not obtain access to any Wikimedia HTTP or HTTPS communications (or communications of any kind), unless users communicating with its websites had been assigned a targeted (whitelisted) IP address. Conversely, if at a given link the NSA were, at its request, not being given access to traffic to or from the IP addresses of certain high-volume but perhaps low-interest sites (blacklisting), such as, hypothetically, Amazon.com, and Wikimedia's sites, then under this scenario, as well, the NSA would receive no access to Wikimedia HTTP or HTTPS communications (or, for that matter, Wikimedia communications of any kind).

82. Regarding the email (SMTP) communications in Category 1, the chart of technical statistics provided by Wikimedia states that the volume of these email communications and the countries from which they are received are unknown. There is no basis, then, on which to assert that these communications with Wikimedia "almost certainly traverse every international backbone link connecting the United States with the rest of the world," the first of the assumptions on which Wikimedia bases its belief that its communications are intercepted by the NSA. (Paragraph 50, above; Amended Complaint ¶ 60) Because the SMTP communications do not satisfy this condition for interception under Wikimedia's own theory, further discussion of these communications is unnecessary for present purposes. Nevertheless, I observe that because all of these communications are received at a sub-set of the same IP addresses as the HTTP and HTTPS communications in Category 1 (as shown in Wikimedia's technical statistics chart), then whitelisting or blacklisting by IP address, as discussed in paragraphs 80-81, above, would also block NSA access to these Wikimedia SMTP email communications as well.

83. Category 2 (server log communications): Wikimedia's technical statistics chart describes the second category of its allegedly intercepted communications, "Wikimedia's internal log communications," as "Apache Kafka log communications" transmitted from Wikimedia servers in the Netherlands to Wikimedia servers in the United States. (Apache Kafka is a commercial data-streaming software application.) These are communications containing server logs, files automatically created and maintained by servers of the activities they perform. A

common example are logs maintained by web servers of user requests to view or download information from a website. These logs typically contain such information as the user's IP address, the time and date of the request, the webpage requested, and the amount of data transmitted. Server logs may be analyzed in aggregate to study traffic patterns, ensure adequate site resources, maintain efficient site administration, and for other purposes. When, as is common, server logs are transmitted elsewhere (to another server) for the performance of such analyses, they are typically encrypted, for security. According to the Amended Complaint, the log communications at issue here are of server logs created by Wikimedia web servers when they receive requests from users seeking to access Wikimedia websites. (Amended Complaint ¶ 93) Wikimedia's technical statistics chart indicates that it encrypts its log communications using an encryption protocol known as IPSec.

84. If the NSA did not wish in the course of Upstream collection to have access to Wikimedia's server log communications, or those of the many other entities that generate such logs, due to their aggregate volume and the relatively limited amount of information they offer (especially if indecipherably encrypted), then it would be a simple matter to block NSA access to those communications, in either of two ways. First, packets encrypted using the IPSec protocol are easily recognized by the corresponding protocol number, protocol 50, contained in their header information. It would be a simple matter at any given link for an assisting carrier to configure the access control list to the interface between its router or switch and a (hypothetical) set of NSA collection equipment to blacklist, that is, to block transmission of, all packets containing protocol 50 in their headers. Second, as shown in Wikimedia's technical statistics chart, its log communications are received at one of the same public IP address ranges as its HTTP, HTTPS, and SMTP communications in Category 1. Like those communications, NSA access to Wikimedia's log communications could be blocked by whitelisting or blacklisting by IP address, as discussed in paragraphs 80-81, above.

85. Category 3 (staff communications): The third and final category of Wikimedia's allegedly intercepted communications, "Communications by Wikimedia staff," are described in

the technical statistics chart as "[l]ogged international" TCP, UDP, and ICMP "connections" using Wikimedia's Office Network or its Virtual Private Network (VPN). "TCP" refers to the Transmission Control Protocol, discussed in paragraph 27, which operates at the transport layer, just beneath the application layer, and allows two devices on the Internet (such as a web server and a user's computer) to establish a connection with one another and exchange streams of data. "UDP" stands for the User Datagram Protocol, another transport layer protocol typically used with applications for which speed is more critical than reliability, such as Internet telephony and video streaming. "ICMP" is the Internet Control Message Protocol, a network layer protocol used by network devices such as routers and servers to send error messages (such as "host unreachable") to other devices when problems are encountered delivering packets.

86. Wikimedia's technical statistics chart does not identify the applications (email, web browsing, VoIP, etc.) used in connection with the TCP and UDP communications identified in Category 3, and so it is unclear whether they are identifiable by port or protocol number. Although the chart specifies that communications conducted over Wikimedia's Virtual Private Network are encrypted using the SSL/TLS protocol described in paragraph 42, it indicates further that not all of its staff communications are sent or received over the encrypted VPN.

87. Nevertheless, the technical statistics chart indicates that Wikimedia's encrypted and unencrypted staff communications are sent from and received at IP addresses that are readily ascertainable from publicly available sources. The IP address range stated for Wikimedia's unencrypted Office Network, 198.73.209.0/24, is discoverable from such sources as the Hurricane Electric directory (see paragraph 80, above, and referenced search results for Wikimedia). (The notation 198.73.209.0/24 in the Hurricane Electric table encompasses the addresses from 198.73.209.0 through 198.73.209.255, and thus includes the address 198.73.209.25 listed as the VPN address in Exhibit 1.) In other words, Wikimedia's staff communications, like its HTTP, HTTPS, and SMTP communications in Category 1, and its log communications in Category 2, could be blocked by whitelisting or blacklisting by IP address, as discussed in paragraphs 80-81, above.

88. In short, at any given Internet backbone link where the NSA might hypothetically be conducting Upstream-type surveillance in a manner posited by Wikimedia, it would be technically feasible for the assisting carrier, through one or more of the traffic-mirroring techniques I have discussed, to configure its routing or switching equipment so that Wikimedia's communications transiting that link are not intercepted, copied, or forwarded to surveillance equipment under the NSA's control.

RELEVANCE OF THE NUMBER OF SITES AT WHICH UPSTREAM SURVEILLANCE OCCURS

89. Finally, I briefly address the import of Wikimedia's assertion that the NSA "must conduct Upstream surveillance at many different backbone chokepoints" if it is to "comprehensively and reliably obtain" communications involving its targets. (Amended Complaint ¶ 66) Wikimedia says this must be true because communications to and from individual targets "may take multiple paths when entering or leaving the United States," even "in the course of a single exchange." (*Id.*) Wikimedia's allegation overstates the extent to which communications between the same two endpoints are likely to take different paths across the Internet, and in particular on Internet backbone networks. As I explained above (paragraph 41), barring network outages or other atypical events, in practice packets transiting between two points on the Internet will follow the same path for the great majority of the distance traveled. The path followed from one communication to the next will differ, if at all, only when the constituent packets first make their way toward the Internet backbone, or as they near their destination.

90. The point is a moot one, though. As I have set out above, at any given backbone link where the NSA might hypothetically be conducting Upstream surveillance in a manner envisioned by Wikimedia, there are various traffic-mirroring techniques available that would allow the NSA, as a technical matter, to obtain access to communications of its targets without intercepting, copying, reviewing, or otherwise interacting with communications of Wikimedia. This would remain the case, therefore, regardless of the number of such locations, whether one, or dozens, at which Upstream surveillance might in theory be conducted.

I declare of penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Executed in New York, New York, on November 12, 2018.

Henning G. Schulzrinne

HENNING G. SCHULZRINNE

DECLARATION OF DR. HENNING G. SCHULZRINNE
***WIKIMEDIA FOUND. V. NSA*, NO. 1:15-CV-00662-TSE (D. MD)**

EXHIBIT A

Henning Schulzrinne

Julian Clarence Levi Professor
Dept. of Computer Science
Columbia University
New York, NY 10027
USA

work phone: +1 212 939 7042
fax: +1 212 666 0140
email: hgs@cs.columbia.edu
WWW: http://www.cs.columbia.edu/~hgs
SIP: sip:hgs@cs.columbia.edu

INTERESTS

Internet multimedia, policy, services, architecture, computer networks and performance evaluation. Telecommunication policy; Internet telephony, collaboration and media-on-demand; Internet of things; emergency services; signaling and session control; mobile applications; ubiquitous and pervasive computing; network measurements; quality of service; Internet protocols and services; congestion control and adaptive multimedia services; implementations of multi-media and real-time networks; operating system support for high-bandwidth services with real-time constraints; performance analysis of computer networks and systems.

WORK EXPERIENCE

Chief Technology Officer, Federal Communications Commission (FCC), January 2017–August 2017.

Senior Advisor for Technology, Federal Communications Commission (FCC), September 2016–December 2016.

Technology Advisor, Federal Communications Commission (FCC), September 2014–August 2016.

Chief Technology Officer, Federal Communications Commission (FCC), January 2012–August 2014.

Engineering Fellow, Federal Communications Commission (FCC), Sept. 2010–May 2011.

Professor (tenured), Dept. of Computer Science and Dept. of Electrical Engineering (joint appointment), Columbia University. August 1996–. Department vice chair, 2002–2003; Department chair, 2004–2009.

Researcher, GMD Fokus[1], Berlin, Germany. March 1994 - July 1996. Multimedia systems, ATM performance issues. Deputy department head; project leader TOMQAT, Multicube, MMTng. Lecturer at Technical University Berlin.

Consultant, 1994-1996: design and implementation of an Internet packet audio tool for a WWW-based "Virtual Places" shared environment (Ubique, Israel). Consultant on real-time packet audio (Vocaltec, Israel).

Postdoc, Distributed Systems Research Department, AT&T Bell Laboratories, Murray Hill, New Jersey. September 1992 – February 1994: designed and implemented BENE network emulator, research in real-time multimedia and electronic publishing.

Teaching Assistant, Dept. of Computer Science, University of Massachusetts, January 1992 – June 1992: co-taught senior-level computer networking course.

Research Assistant, Dept. of Computer Science, University of Massachusetts, July 1988 – September 1992: research in congestion control and performance evaluation related

[1] GMD - Forschungszentrum Informationstechnik (German National Research Center for Information Technology), Research Institute for Open Communication Systems

to high-speed computer networks. Also assisted in teaching performance evaluation course.

Research Assistant, Dept. of Electrical and Computer Engineering, University of Massachusetts at Amherst, January 1988 – July 1988: collaboration with Dr. Wei-Bo Gong in the area of perturbation analysis.

Teaching Assistant, Dept. of Electrical and Computer Engineering, University of Massachusetts at Amherst, September 1987 – July 1988: taught discussion section of introductory programming class for engineers (Pascal and Fortran).

Research Assistant, Dept. of Electrical and Computer Engineering, University of Cincinnati, March 1985 – August 1987: planning and implementation of speech processing laboratory and networking, tool development, vector quantization research, system administration.

EDUCATION

PhD Electrical Engineering, Department of Electrical and Computer Engineering at the University of Massachusetts, Amherst, September 1992.

PhD Thesis: *Congestion Control and Packet Loss for Real-Time Traffic in High-Speed Networks*. Principal advisors: Jim Kurose, Don Towsley and Christos Cassandras.

Master of Science, Department of Electrical and Computer Engineering at the University of Cincinnati, Cincinnati, Ohio; with emphasis on digital signal processing (voice coding, software models). August 1987.

Master's thesis: *Multi-Stage Vector Quantization for Speech and Image Coding; The DSP Workbench: Distributed Multiprocess System Simulation*. Experimental and theoretical results for a new method of vector quantization and development of a distributed high-level simulator for signal processing applications. Principal advisor: P. A. Ramamoorthy.

B.S. Electrical Engineering, (combined with B.S. Industrial Engineering), Technical University of Darmstadt, Federal Republic of Germany, June 1984.

HONORS AND AWARDS

- IEEE Infocom 2018 *Test of Time Paper Award* for "An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol" (with Salman Baset).
- IEEE Internet award, 2016.
- ACM Fellow, 2015.
- WCNC 2015, "Intelligent Content Delivery over Wireless via SDN", best paper award.
- IEEE Communications Society Internet Technical Committee Distinguished Service Award, 2014.
- Internet Hall of Fame, 2013
- GREE 2013 best paper award ("Wimax in the classroom: Designing a cellular networking hands-on lab")
- 2011 Internet2 IDEA Award winner for "Do You See What I See" tool (Kyung Hwa Kim, PhD Student)
- Region 1 William Terry Award for Lifetime Distinguished Service to IEEE Region 1 (2010)

- IPTComm 2010 best paper award ("Reliability and Relay Selection in Peer-to-Peer Communication Systems")
- IMSAA-08 3rd best paper award for *A New SIP Event Package For Group Membership Management in Advanced Communications* (co-authored with Vishal Singh and Piotr Boni)
- VDE ITG Preis 2008 for *Ubiquitous Device Personalization and Use: The Next Generation of IP Multimedia Communications* (co-authored with Ron Shacham, Srisakul Thakolsri and Wolfgang Kellerer)
- IPTCOMM 2008 Best Student Paper Award for *SIP Server Overload Control: Design and Evaluation* (co-authored with Charles Shen)
- CATT lifetime innovation award (Brooklyn Polytech University) (2007)
- Sputnik Innovator Award (2005)
- IEEE Fellow (2006)
- IEEE ComSoc Technical Committee on Computer Communications (TCCC) Outstanding Service Award 2005
- IEEE Senior Member (2004)
- Internet Telephony 2004 Product of the Year
- Mayor's Award for Excellence in Science and Technology (2004)
- VON Pioneer Award, 2000
- *IEEE Communication Society* Lecturer, 1997
- nominated for ACM Best Dissertation award
- University of Massachusetts Graduate School Fellowship, 1990-1991
- University Summer Research Fellowship 1987
- University Summer Research Fellowship 1985
- German Fulbright Scholarship 1984
- President Electrical Engineering Graduate Student Association 1985/86
  Graduate Outstanding Service award 1986
- German National Scholarship Foundation ("Studienstiftung des deutschen Volkes")
- Regional finalist German Young Scientists Competition (Jugend forscht)

PROFESSIONAL ACTIVITIES

Editorial positions:

- Associate Editor, *Computer Communications*, 2009–
- Editor, *Foundations and Trends in Networking*, 2005–.
- Editor, *ACM Transactions on Multimedia Computing, Communications and Applications*, 2005–
- Associate Editor, *ACM/IEEE Transactions on Networking*, 2000–2008
- Associate Editor, *IEEE Transactions on Image Processing*, 1999–2000
- Guest editor for *IEEE Network Magazine* and *IEEE Internet Computing* on Internet Telephony, May/June 1999
- *Journal of Communications and Networks*, editor (1998–2001), division editor (2001–2004)

- *IEEE Communication Surveys*, member editorial board, 1996–2000, 2002–
- *Internet Computing*, Communications Society liaison editor, 1996–1999, editor, 2008–
- *IEEE Communications Magazine*, Internet Technology feature series editor (1996–1998)
- Guest editor for *IEEE Journal on Selected Areas in Communications* on the Global Internet

Technical program committees:

- *P2P* 2008
- *ANCS (Architectures for Networking and Communication Systems)* 2005
- *ACM Multimedia* 2005
- *SIP 2000–2008*
- *Feature Interaction Workshop (FIW)* 2003, 2005
- *International Conference on Distributed Computing Systems (ICDCS)* 2005
- *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks* (WoWMoM) 2005, 2006
- ACM *Mobihoc* 2002, 2005
- IEEE *INFOCOM* 1994–1996, 1998, 2000–2004, 2006–2019
- *Network and Operating System Support for Digital Audio and Video* (NOSSDAV), 1997–2010, 2012–2014
- *IEEE Global Internet* 1996–2000, 2005, 2007
- *Packet Video Workshop*, 1999, 2000
- *ACM/SPIE Multimedia Computing and Networking*, 1998
- *Open Architectures and Network Programming (OPENARCH)* 1998, 1999
- NSF review panel, 1999, 2002, 2003, 2004, 2006, 2007, 2008, 2010, 2011, 2015
- *IEEE Global Internet*, November 1996 (conference technical program vice chair)
- W3C *Real-Time Multimedia Workshop* (RTMW), October 1996
- *International Conference on Network Protocols (ICNP)*, 1996, 2008
- *Workshop on Integration of IP and ATM*, 1996

Advisory boards and committees:

- North American Numbering Council (NANC), a federal advisory committee (FCC, 2017–2018)
- Computing Community Consortium, Intelligent Infrastructure Task Force (2017–2018)
- Applied Technology Council (ATC) - ATC-126 (*Community Resilience of Lifeline Systems*) project technical committee (2016)
- Steering Committee (member, current chair), *IEEE/ACM Transactions on Networking* (2007–2017)
- ACM publication board technology committee (2015)
- ACM SIGCOMM vice chair (2007–2013)
- Member of the Board, Armstrong Memorial Research Foundation (2009–)

- Internet2 Applications, Middleware and Services Advisory Council (AMSAC) (2008–2012)
- GENI OptIn working group co-chair (2008–2009)
- board of directors, *SIP Forum* (1998–2002)
- Member of Internet Architecture Board (IAB), the technical advisory group of the Internet Society and the architectural oversight body of the IETF (1999–2001)
- Co-chair, *Internet Technical Committee* of the IEEE Communications Society (1994-2000)
- Chair, *IEEE Communications Society Technical Committee on Computer Communications* (1999–2001)
- SIP Bake-Offs, Columbia University (April 1999, August 1999, December 1999)
- IEEE *Infocom* Executive Committee (1995–2000)
- Internet2 Applications, Middleware and Services Advisory Council (AMSAC) 2008–2010
- GENI OptIn working group co-chair, 2008–2009
- IEEE Travel Reduction Task Force, 2009
- member-at-large, Board of Governors, IEEE *Communications Society*, 2002
- board of directors, *SIP Forum*, 1998–2002
- past co-Chair, *Internet Technical Committee* of the IEEE Communications Society
- Chair, *IEEE Communications Society Technical Committee on Computer Communications* (1999–2001)
- member IEEE Electronic Processes Steering Group, 2000

Conference leadership:

- *Mobiquitous 2018* general co-chair
- *e-Energy 2011* technical program co-chair
- *IEEE COMSNETS 2010* general co-chair
- *IEEE P2P 2009* general co-chair
- *IEEE ICNP 2009* general co-chair
- *IFIP Networking 2009* technical program co-chair
- *IEEE IM 2009* technical program co-chair
- *ACM IPTCOMM 2008* technical program co-chair
- *ACM IPTCOMM 2007* general co-chair
- *CoNext 2007* general co-chair
- *ACM Multimedia* 2004 general co-chair
- technical program co-chair Internet Telephony Workshop 2001
- IEEE *Infocom* 2000 technical program co-chair
- *NOSSDAV* technical program co-chair 2001
- IEEE *Infocom* 1998 vice general chair
- Organizer, SIP Bake-Offs, Columbia University (April 1999, August 1999, December 1999)

- IEEE *Infocom* Executive Committee 1995–2000
- *NOSSDAV*, *MobiArch* and *IPTComm* steering committees (current)

Referee for *IEEE Transactions on Networking*, *Springer/ACM Multimedia Systems Journal*, *IEEE Transactions on Communications*, *Computer Networks and ISDN Systems*, *Internetworking*, IEEE Infocom, ACM Sigcomm, IC^{3}N, National Science Foundation, and others.

Maintainer and editor of the web-based Network Bibliography.

PATENTS

US patent 5,509,074: *Method of protecting electronically published materials using cryptographic protocols* (issued April 1996)

US patent 6,141,788: *Method And Apparatus For Forward Error Correction In Connection In Packet Networks* (October 2000)

US patent 6,446,108: *Method For Network Address Translation* (September 2002)

US patent 6,538,416: *Border Gateway Reservation Protocol for Tree-Based Aggregation of Inter-Domain Reservations* (March 2003)

US patent 6,771,644: *Program insertion in real time IP multicast* (August 2004)

US patent 6,937,597: *Signaling Method For Internet Telephony* (August 2005)

US patent 6,970,909: *Multi-protocol data communication systems supporting wireless telephony and content delivery* (November 2005)

US patent 7,257,201: *System and method for unified messaging in inter/intranet telephony* (August 2007)

US patent 7,266,091: *System and method for conferencing in inter/intranet telephony* (September 2007)

US patent 7,296,091: *System and method for receiving over a network a broadcast from a broadcast source* (November 2007)

US patent 7,319,689: *Method for handling the simultaneous mobility of mobile hosts in infrastructure-based networks* (January 2008)

US patent 7,610,384: *Network telephony appliance and system for inter/intranet telephony* (October 2009)

US patent 7,610,384: *Network telephony appliance and system for inter/intranet telephony* (October 2009)

US patent 7,636,336 *Methods and systems for reducing MAC layer handoff latency in wireless networks* (December 2009)

US patent 8,027,251 *Systems and methods for implementing protocol-aware network firewall* (September 2011)

US patent 8,166,102 *Signaling method for internet telephony* (April 2012)

US patent 8,302,186 *System and method for testing network firewall for denial-of-service (DOS) detection and prevention in signaling channel* (October 2012)

US patent 8,522,344 *Theft of service architectural integrity validation tools for session initiation protocol (SIP)-based systems* (August 2013)

US patent 8,565,384 *Systems, methods, and media for connecting emergency communications* (October 2013)

US patent 8,689,328 *Malicious user agent detection and denial of service (DOS) detection and prevention using fingerprinting* (March 2014)

US patent 8,719,926 *Denial of service detection and prevention using dialog level filtering* (April 2014)

US patent 8,737,220 *Systems for providing feedback to sending entities* (May 2014)

US patent 8,737,351 *Methods and systems for reducing MAC layer handoff latency in wireless networks* (May 2014)

US patent 8,750,242 *Methods, media, and devices for moving a connection from one point of access to another point of access* (June 2014)

US patent 8,804,513 *Methods and systems for controlling SIP overload* (August 2014)

US patent 8,966,619 *Prevention of denial of service (DoS) attacks on session initiation protocol (SIP)-based systems using return routability check filtering* (February 2015)

US patent 8,995,742 *Methods and systems for controlling traffic on a communication network* (March 2015)

US patent 9,036,605 *Methods, media, and devices for moving a connection from one point of access to another point of access* (May 2015)

US patent 9,118,814 *Set-top box peer-assisted video-on-demand* (August 2015)

US patent 9,374,342 *System and method for testing network firewall using fine granularity measurements* (June 2016)

US patent 8,750,242 *Methods, media, and devices for moving a connection from one point of access to another point of access* (July 2016)

US patent 9,473,529 *Prevention of denial of service (DoS) attacks on Session Initiation Protocol (SIP)-based systems using method vulnerability filtering* (October 2016)

US patent 10,039,033 *Systems, methods, and media for implementing call handoff between networks* (July 2018)

TUTORIALS

Partial listing:

- *IDMS/PROMS*, Coimbra, November 2002;
- *Mobicom* tutorial, Atlanta, September 2002;
- *Sigcomm* tutorial, Stockholm, August 2000;
- *International Conference on Multimedia (ICME)*, July 2000;
- *Networking 2000* tutorial, Paris, May 2000;
- *IEEE Real Time Applications Symposium*, May 2000;
- *VON Developers Conference*, semi-annually since 1999;
- BellSouth (Atlanta), February and March 1998, November 1999;
- *IEEE International Conference on Network Protocols* (ICNP), October 1999;
- ASSET conference (Dallas, Texas), March 1999;
- CEFRIEL (Milan), May 1999;
- MCI Corp. (Colorado Springs), August 1998;
- EPFL summer school (Lausanne, Switzerland), June 1998;

- 16th Brazilian Symposium on Computer Networks, May 1998;
- IEEE Infocom, March 1998;

SOFTWARE

MICE: Web-based information management for departmental personnel, student, space and financial data;

CINEMA: Columbia InterNet Extensible Multimedia Architecture (with Jonathan Lennox, Kundan Singh, and others);

EDAS: editor's assistant; conference paper management software used for IEEE ICC, IEEE Globecom, Mobicom, IEEE Infocom, ICNP, NOSSDAV, Packet Video (about 8,000 total), with roughly 770,000 users;

e*phone: Ethernet packet audio device; the first SIP-speaking embedded Internet phone (with Jianqi Yin).

graph++: graphing tool with matrix manipulation facilities.

NeVoT: network voice terminal, first RTP-capable Internet voice application.

rtptools: set of tools for analyzing, recording and playing back RTP packets; used in a number of media-on-demand projects.

RTP library: library implementing RTP (with Jonathan Lennox, Jonathan Rosenberg and Dan Rubenstein);

rtspd: RTSP multimedia server (with Jonathan Lennox and Kundan Singh).

sipc: SIP user agent (Internet telephony agent) (with Xiaotao Wu).

sipconf: SIP-based software conferencing server (with Kundan Singh);

sipd: First publically available SIP proxy and redirect server (with Jonathan Lennox);

sipum: SIP-based unified messaging system (with Kundan Singh);

simul: discrete-event simulator emulating SIMAN.

JOURNAL PUBLICATIONS

[1] H. Schulzrinne, "Network neutrality is about money, not packets (invited paper)," *IEEE Internet Computing*, Vol. 22, November/December 2018.

[2] H. Schulzrinne, "Networking research – a reflection in the middle years (invited paper)," *Computer Communications*, 2018.

[3] S. G. Hong, S. Seo, H. Schulzrinne, and P. Chitrapu, "ICOW: Internet access in public transit systems," *IEEE Communications Magazine*, Vol. 53, pp. 134–141, June 2015.

[4] M. Berman, P. Demeester, J. W. Lee, K. Nagaraja, M. Zink, D. Colle, D. K. Krishnappa, D. Raychaudhuri, H. Schulzrinne, I. Seskar, and S. Sharma, "Future internets escape the simulator," *Communications ACM*, Vol. 58, pp. 78–89, May 2015.

[5] E. Piri and H. Schulzrinne, "Scaling network information services to support hetnets and dynamic spectrum access," *Journal of Communications and Networks*, Vol. 16, Apr. 2014.

[6] S. G. Hong and H. Schulzrinne, "PBS: Signaling architecture for network traffic authorization," *IEEE Communications Magazine*, Vol. 51, pp. 89–96, July 2013.

[7] O. Boyaci, V. Beltran, and H. Schulzrinne, "Bridging communications and the physical world," *IEEE Internet Computing*, Vol. 16, no. 2, pp. 35–43, 2012.

[8] D. Touceda, J. Sierra, A. Izquierdo, and H. Schulzrinne, "Survey of attacks and defenses on P2PSIP communications," *IEEE Communications Surveys Tutorials*, Vol. 14, no. 3, pp. 750–783, 2012.

[9] C. Shen, E. Nahum, H. Schulzrinne, and C. P. Wright, "The impact of TLS on SIP server performance: Measurement and modeling," *IEEE/ACM Transactions on Networking*, Vol. 20, pp. 1217–1230, Aug. 2012.

[10] J. Kayfetz, H. Schulzrinne, T. Sherwood, and M. Tiwari, "Your desktop or mine: Extending the reach of writing instruction," *Ubiquitous Learning*, Vol. 3, no. 3, 2011.

[11] E. Brosh, S. A. Baset, V. Misra, D. Rubenstein, and H. Schulzrinne, "The Delay-Friendliness of TCP for Real-Time traffic," *IEEE/ACM Transactions on Networking*, Oct. 2010.

[12] H. Tschofenig and H. Schulzrinne, "Emergency services for internet multimedia," *The Internet Protocol Journal*, Dec. 2010.

[13] S. Subramanya, X. Wu, H. Schulzrinne, and S. Buriak, "VoIP-based air traffic controller training," *IEEE Communications Magazine*, Nov. 2009.

[14] S. Alexander, Y.-H. Cheng, B. Coan, A. Ghetie, V. Kaul, B. Siegell, S. Bellovin, N. Maxemchuk, and H. Schulzrinne, "The dynamic community of interest and its realization in ZODIAC," *IEEE Communications Magazine*, Oct. 2009.

[15] H. Schulzrinne, "Double submissions: publishing misconduct or just effective dissemination?," *CCR*, July 2009.

[16] H. Schulzrinne, "Double-blind reviewing: more placebo than miracle cure?," *CCR*, Apr. 2009.

[17] S. Shin and H. Schulzrinne, "Measurement and analysis of the VoIP capacity in IEEE 802.11 WLAN," *IEEE Transactions on Mobile Computing*, Sept. 2009.

[18] R. Dantu, S. Fahmy, H. Schulzrinne, and J. Cangussu, "Issues and challenges in securing VoIP," *Computers & Security*, May 2009.

[19] X. Fu, H. Schulzrinne, H. Tschofenig, C. Dickmann, and D. Hogrefe, "Overhead and performance study of the general internet signaling transport (GIST) protocol," *IEEE/ACM Transactions on Networking*, Feb. 2009.

[20] D. Chopra, H. Schulzrinne, E. Marocco, and E. Ivov, "Peer-to-peer overlays for real-time communication: security issues and solutions," *IEEE Communications Surveys & Tutorials*, Jan. 2009.

[21] H. Schulzrinne, "Conferences as organizations: advising, steering and establishing expectations," *ACM SIGCOMM Computer Communication Review*, Jan. 2009.

[22] G. Camarillo, H. Schulzrinne, S. Loreto, and J. Hautakorpi, "Effect of head of the line blocking on session initiation protocol session establishment delays," *Journal of Communications and Networks*, Feb. 2009.

[23] S. G. Hong, V. Hilt, and H. Schulzrinne, "Evaluation of control message overhead of DHT-based P2P system," *Bell Labs Technical Journal*, Nov. 2008.

[24] A. Dutta, D. Famolari, S. Das, Y. Ohba, V. Fajardo, K. Taniuchi, R. Lopez, and H. Schulzrinne, "Media-independent pre-authentication supporting secure interdomain handover optimization," *IEEE Wireless Communications*, Apr. 2008.

[25] X. Wang and H. Schulzrinne, "Measurement and analysis of LDAP performance," *IEEE/ACM Transactions on Networking*, Feb. 2008.

[26] K. Arabshian and H. Schulzrinne, "An ontology-based hierarchical Peer-to-Peer global service discovery system," *Journal of Ubiquitous Computing and Intelligence (JUCI)*, Vol. 1, pp. 133–144, Dec. 2007.

[27] W. Yuen and H. Schulzrinne, "Improving search efficiency using bloom filters in partially connected ad hoc networks: A node-centric analysis," *Computer Communications*, Nov. 2007.

[28] A. Dutta, S. Das, D. Famolari, Y. Ohba, K. Taniuchi, V. Fajardo, R. M. Lopez, T. Kodama, and H. Schulzrinne, "Seamless proactive handover across heterogeneous access networks," *Wireless Personal Communications*, Nov. 2007.

[29] R. Shacham, H. Schulzrinne, S. Thakolsri, and W. Kellerer, "Ubiquitous device personalization and use: The next generation of IP multimedia communications," *ACM Transactions on Multimedia Computing, Communications, and Applications*, Aug. 2007.

[30] R. Dantu, D. Ghosal, and H. Schulzrinne, "Securing voice over IP," *IEEE Network*, Vol. 20, pp. 4–5, Sept. 2006.

[31] X. Wang and H. Schulzrinne, "Pricing network resources for adaptive applications," *IEEE/ACM Transactions on Networking*, Vol. 14, pp. 506–519, June 2006.

[32] K. Wong, A. Dutta, H. Schulzrinne, and K. Young, "Simultaneous mobility: analytical framework, theorems, and solutions," *Wireless Communication and Mobile Computing*, June 2006.

[33] K. Singh and H. Schulzrinne, "Failover, load sharing and server architecture in SIP telephony," *Computer Communications*, Mar. 2007.

[34] W. Zhao and H. Schulzrinne, "Enhancing service location protocol for efficiency, scalability and advanced discovery," *The Journal of Systems & Software*, Vol. 75, pp. 193–204, Feb. 2005.

[35] X. Wang and H. Schulzrinne, "Incentive-Compatible adaptation of internet Real-Time multimedia," *IEEE Journal on Selected Areas in Communications*, Vol. 23, pp. 417–436, Feb. 2005.

[36] W. Kellerer, M. Wagner, W.-T. Balke, and H. Schulzrinne, "Preference-based session management for IP-based mobile multimedia signaling," *European Transactions on Telecommunications*, Vol. 15, pp. 415–427, Aug. 2004.

[37] L. Amini, A. Shaikh, and H. Schulzrinne, "Issues with inferring internet topological attributes," *Computer Communications*, Vol. 27, pp. 557–567, Apr. 2004.

[38] P. Mendes, H. Schulzrinne, and E. Monteiro, "How to increase the efficiency of receiver-driven adaptive mechanisms in a new generation of IP networks," *Computer Communications*, Vol. 27, pp. 345–354, Feb. 2004.

[39] A. Dutta and H. Schulzrinne, "MarconiNet: overlay mobile content distribution network," *IEEE Communications Magazine*, Feb. 2004.

[40] H. Schulzrinne, X. Wu, S. Sidiroglou, and S. Berger, "Ubiquitous computing in home networks," *IEEE Communications Magazine*, pp. 128–135, Nov. 2003.

[41] D. Wong, A. Dutta, J. Burns, K. Young, and H. Schulzrinne, "A multilayered mobility management scheme for auto-configured wireless IP networks," *IEEE Wireless Magazine*, Oct. 2003.

[42] A. Dutta, J. Chennikara-Varghese, W. Chen, O. Altintas, and H. Schulzrinne, "Multicasting streaming media to mobile users," *IEEE Communications Magazine*, Oct. 2003.

[43] P. Mendes, H. Schulzrinne, and E. Monteiro, "How to increase the efficiency of receiver-driven adaptive mechanisms in a new generation of IP networks," *Computer Communications*, Vol. 26, 2003.

[44] G. Camarillo, H. Schulzrinne, and R. Kantola, "Evaluation of transport protocols for the session initiation protocol," *IEEE Network*, 2003.

[45] P. Mendes, H. Schulzrinne, and E. Monteiro, "Session-aware popularity resource allocation for assured differentiated services," *IEEE Communications Magazine*, Sept. 2002.

[46] J. Brassil and H. Schulzrinne, "Enhancing Internet streaming media with cueing protocols," *IEEE/ACM Transactions on Networking*, Vol. 10, Aug. 2002.

[47] H. Schulzrinne and K. Arabshian, "Providing emergency services in Internet telephony," *IEEE Internet Computing*, Vol. 6, pp. 39–47, May 2002.

[48] W. Jiang, J. Lennox, S. Narayanan, H. Schulzrinne, K. Singh, and X. Wu, "Integrating Internet telephony services," *IEEE Internet Computing*, Vol. 6, pp. 64–72, May 2002.

[49] H. Schulzrinne, "Internet telefonie – mehr als nur ein telefon mit paketvermittlung," *PIK – Praxis der Informationsverarbeitung und Kommunikation*, Vol. 24, Jan. 2001.

[50] X. Wang and H. Schulzrinne, "An integrated resource negotiation, pricing, and QoS adaptation framework for multimedia applications," *IEEE Journal on Selected Areas in Communications*, Vol. 18, pp. 2514–2529, Dec. 2000.

[51] H. Schulzrinne and J. Rosenberg, "The session initiation protocol: Internet-centric signaling," *IEEE Communications Magazine*, Vol. 38, Oct. 2000.

[52] H. Schulzrinne and E. Wedlund, "Application-layer mobility using SIP," *Mobile Computing and Communications Review (MC2R)*, Vol. 4, pp. 47–57, July 2000.

[53] P. Pan, E. Hahne, and H. Schulzrinne, "The border gateway reservation protocol (BGRP) for tree-based aggregation of inter-domain reservations," *Journal of Communications and Networks*, June 2000.

[54] X. Wang and H. Schulzrinne, "Comparison of adaptive Internet multimedia applications," *IEICE Transactions on Communications*, June 1999.

[55] C. A. Polyzois, K. H. Purdy, P. Q. Yang, D. C. Shrader, H. Sinnreich, F. Ménard, and H. Schulzrinne, "From POTS to PANS – a commentary on the evolution to Internet telephony," *IEEE Network*, Vol. 13, pp. 58–64, May/June 1999.

[56] J. Rosenberg and H. Schulzrinne, "The IETF Internet telephony architecture and protocols," *IEEE Network*, Vol. 13, pp. 18–23, May/June 1999.

[57] J. Rosenberg, J. Lennox, and H. Schulzrinne, "Programming Internet telephony services," *IEEE Network*, Vol. 13, pp. 42–49, May/June 1999.

[58] P. Pan and H. Schulzrinne, "YESSIR: a simple reservation mechanism for the Internet," *ACM Computer Communication Review*, Vol. 29, pp. 89–101, Apr. 1999.

[59] J. Brassil, S. Garg, and H. Schulzrinne, "Program insertion in real-time IP multicasts," *ACM Computer Communication Review*, Vol. 29, pp. 49–68, Apr. 1999.

[60] H. Schulzrinne and J. Rosenberg, "Internet telephony: Architecture and protocols – an IETF perspective," *Computer Networks and ISDN Systems*, Vol. 31, pp. 237–255, Feb. 1999.

[61] H. Schulzrinne and J. Rosenberg, "The session initiation protocol: Providing advanced telephony services across the Internet," *Bell Labs Technical Journal*, Vol. 3, pp. 144–160, October-December 1998.

[62] H. Schulzrinne, "Transatlantische netze," *DFN Mitteilungen*, Vol. 46, pp. 23–24, Mar. 1998.

[63] D. Sisalem and H. Schulzrinne, "The multimedia Internet terminal (mint)," *Telecommunications Systems*, Vol. 9, pp. 423–444, Sep 1998.

[64] H. Schulzrinne, "Operating system issues for continuous media," *Multimedia Systems*, Vol. 4, pp. 269–280, Oct. 1996.

[65] H. Schulzrinne, "World-wide web: Whence, whither, what next?," *IEEE Network*, Vol. 10, pp. 10–17, March/April 1996.

[66] I. Busse, B. Deffner, and H. Schulzrinne, "Dynamic QoS control of multimedia applications based on RTP," *Computer Communications*, Vol. 19, pp. 49–58, Jan. 1996.

[67] J. Crowcroft, D. Estrin, H. Schulzrinne, and M. Schwartz, "Guest editorial: The global Internet," *IEEE Journal on Selected Areas in Communications*, Vol. 13, pp. 1366–1369, Oct. 1995.

[68] H. Schulzrinne, "Conferencing and collaborative computing: Where are we?," *it+ti (Informationstechnik und Technische Informatik)*, Vol. 37, pp. 58–63, Aug. 1995.

[69] J. P. Sterbenz, H. Schulzrinne, and J. D. Touch, "Report and discussion on the IEEE comsoc TCGN gigabit networking workshop 1995," *IEEE Network*, Vol. 9, pp. 9–21, July/August 1995.

[70] H. Schulzrinne, "IPv6 – the new Internet protocol," *PIK – Praxis der Informationsverarbeitung und Kommunikation*, Vol. 18, pp. 165–167, July-September 1995.

[71] A. K. Choudhury, N. F. Maxemchuk, S. Paul, and H. Schulzrinne, "Copyright protection for electronic publishing over computer," *IEEE Network*, Vol. 9, pp. 12–20, May/June 1995.

[72] Çaglan M. Aras, J. F. Kurose, D. Reeves, and H. Schulzrinne, "Real-time communications in packet-switched networks," *Proceedings of the IEEE*, Vol. 82, pp. 122–139, Jan. 1994.

[73] W.-B. Gong and H. Schulzrinne, "Application of smoothed perturbation analysis to probabilistic routing," *Mathematics and Computers in Simulation*, Vol. 32, pp. 467–485, 1992.

BOOKS AND CHAPTERS

[1] A. Dutta and H. Schulzrinne, *Mobility Protocols and Handover Optimization: Design, Evaluation and Application*. Chichester: John Wiley, 2014.

[2] H. Tschofenig and H. Schulzrinne, *Internet Protocol-based Emergency Services*. Chichester: Wiley, 2013.

[3] M. Papadopouli and H. Schulzrinne, *Peer-to-Peer Computing for Mobile Networks*. Springer, Jan. 2009.

[4] D. Sisalem, J. Floroiu, J. Kuthan, U. Abend, and H. Schulzrinne, *SIP Security*. Wiley, May 2009.

[5] T. Chiba, H. Yokota, A. Idoue, A. Dutta, K. Manousakis, S. Das, and H. Schulzrinne, "Trombone routing mitigation techniques for IMS/MMD networks," in *IEEE Wireless Communications and Networking Conference 2007 - Networking*, (Hong Kong, Hong Kong), Mar. 2007.

[6] A. Dutta, H. Schulzrinne, and K. Wong, *Supporting Continuous Services to Roaming Clients*, ch. 17. USA: CRC, 2006.

[7] H. Schulzrinne, "Internet telephony," in *Practical Handbook of Internet Computing*, CRC, 2004.

[8] K. Wong, H.-Y. Wei, A. Dutta, K. Young, and H. Schulzrinne, "IP micro-mobility management using host-based routing," in *Wireless IP and building the Mobile Internet* (S. Dixit and R. Prasad, eds.), Artech House, 2002.

[9] H. Schulzrinne, "IP networks," in *Compressed Video Over Networks* (A. Reibman and M.-T. Sun, eds.), Marcel Dekker, 2001.

[10] R. Guérin and H. Schulzrinne, "Network quality of service," in *Grid: Blueprint for a New Computing Infrastructure* (I. Foster and C. Kesselman, eds.), San Francisco, California: Morgan Kaufmann Publishers, 1998.

[11] H. Schulzrinne, "Operating system issues for continuous multimedia," in *Handbook of Multimedia Computing* (B. Furht, ed.), pp. 627–648, Boca Raton: CRC Press, 1998.

CONFERENCE PUBLICATIONS

[1] V. Gadiraju, A. Panat, R. Poddar, Z. Sherriff, S. Kececi, and H. Schulzrinne, "Who gets broadband when? A panel data analysis of demographic, economic and technological factors explaining U.S. broadband deployment," in *TPRC46: Research Conference on Communications, Information and Internet Policy*, (Washington, DC), Sept. 2018.

[2] W. Falcon and H. Schulzrinne, "Predicting floor-level for 911 calls with neural networks and smartphone sensor data," in *Sixth International Conference on Learning Representations*, (Vancouver, Canada), Apr. 2018.

[3] J. Janak and H. Schulzrinne, "Framework for rapid prototyping of distributed IoT applications powered by WebRTC," in *Proc. of IPTComm 2016*, (Chicago, Illinois), Oct. 2016.

[4] H. Nam, K. H. Kim, and H. Schulzrinne, "QoE matters more than QoS: why people stop watching cat videos," in *IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications (INFOCOM 2016)*, (San Francisco, USA), pp. 847–855, Apr. 2016.

[5] K. H. Kim, J. W. Lee, M. Ben-Ami, H. Nam, J. Janak, and H. Schulzrinne, "Flexible network address mapping for container-based clouds," in *First IEEE Conference on Network Softwarization 2015 (NetSoft 2015)*, (London, United Kingdom), Apr. 2015.

[6] H. Nam, D. Calin, and H. Schulzrinne, "Intelligent content delivery over wireless via SDN," in *2015 IEEE Wireless Communications and Networking Conference (WCNC)*, (New Orleans, USA), pp. 2203–2208, Mar. 2015.

[7] M. Varela, P. Zwickl, P. Reichl, M. Xie, and H. Schulzrinne, "Experience level agreements (ELA): the challenges of selling QoE to the user," in *IEEE ICC 2015 - Workshop on Quality of Experience-based Management for Future Internet Applications and Services (QoE-FI) (ICC'15 - Workshops 04)*, (London, United Kingdom), June 2015.

[8] H. Nam, K. H. Kim, J. Y. Kim, and H. Schulzrinne, "Towards QoE-aware video streaming using SDN," in *Globecom 2014 - Communications Software, Services and Multimedia Symposium (GC14 CSSM)*, (Austin, USA), pp. 1334–1339, Dec. 2014.

[9] H. Nam, K.-H. Kim, D. Calin, and H. Schulzrinne, "YouSlow: A performance analysis tool for adaptive bitrate video streaming," in *Proc. of SIGCOMM 2014 Posters and Demos*, (Chicago, Illinois), Aug. 2014.

[10] K. H. Kim, H. Nam, V. Singh, D. Song, and H. Schulzrinne, "DYSWIS: Crowdsourcing a home network diagnosis," in *Proc. of 23rd International Conference on Computer Communications and Networks (ICCCN 2104)*, (Shanghai, China), Aug. 2014.

[11] H. Nam, K. H. Kim, D. Calin, and H. Schulzrinne, "Towards dynamic network condition-aware video server selection algorithms over wireless networks," in *19th IEEE Symposium on Computers and Communications (IEEE ISCC 2014)*, (Madeira, Portugal), June 2014.

[12] W. Song, J. W. Lee, B. S. Lee, and H. Schulzrinne, "Finding 9-1-1 callers in tall buildings," in *15th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (IEEE WoWMoM 2014)*, (Sydney, Australia), June 2014.

[13] H. Nam, K. H. Kim, B. H. Kim, D. Calin, and H. Schulzrinne, "Towards dynamic QoS-aware Over-The-Top video streaming," in *15th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (IEEE WoWMoM 2014)*, (Sydney, Australia), June 2014.

[14] K. H. Kim, H. Nam, J. H. Park, and H. Schulzrinne, "MoT: a collaborative network troubleshooting platform for the Internet of things," in *IEEE WCNC'14 Track 4 (Services, Applications, and Business) (IEEE WCNC'14 Track 4: SAB)*, (Istanbul, Turkey), pp. 3461–3466, Apr. 2014.

[15] K. H. Kim, H. Nam, and H. Schulzrinne, "WiSlow: a WiFi network performance troubleshooting tool for end users," in *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications (INFOCOM'2014)*, (Toronto, Canada), pp. 862–870, Apr. 2014.

[16] H. Schulzrinne, "Transitioning the public switched telephone network into the 21st century," in *Proc. of ConTEL (12th International Conference on Telecommunications)*, (Zagreb, Croatia), pp. 3–4, June 2013.

[17] J. Y. Kim and H. Schulzrinne, "Cloud support for latency-sensitive telephony applications," in *Proceedings of the 2013 IEEE International Conference on Cloud Computing Technology and Science*, CLOUDCOM '13, (Bristol, UK), pp. 421–426, IEEE Computer Society, Dec. 2013.

[18] A. Singh, H. Schulzrinne, G. Ormazabal, S. Addepalli, P. Thermos, and Y. Zou, "Unified heterogeneous networking design," in *Principles, Systems and Applications of IP Telecommunications 2013 (IPTComm 2013)*, (Chicago, Illinois, USA), Oct. 2013.

[19] H. Nam, B. H. Kim, D. Calin, and H. Schulzrinne, "A mobile video traffic analysis: Badly designed video clients can waste network bandwidth," in *Globecom*

2013 Workshop - Control Techniques for Efficient Multimedia Delivery (GC13 WS - CTEMD), (Atlanta, USA), pp. 512–517, Dec. 2013.

[20] M. Femminella, G. Reali, D. Valocchi, R. Francescangeli, and H. Schulzrinne, "Advanced caching for distributing sensor data through programmable nodes," in *Proc. of IEEE LANMAN*, (Brussels, Belgium), Apr. 2013.

[21] K.-H. Kim, H. Nam, and H. Schulzrinne, "WiSlow: A performance troubleshooting tool for Wi-Fi networks," in *Proc. of NSDI (poster/demo)*, (Lombard, Illinois), Apr. 2013.

[22] J. Marasevic, J. Janak, H. Schulzrinne, and G. Zussman, "WiMAX in the classroom: Designing a cellular networking hands-on lab," in *Proc. of 2nd GENI Research and Educational Experiment Workshop (GREE2013)*, (Salt Lake City, Utah), Mar. 2013.

[23] W. Song, G. Hampel, A. Rana, T. E. Klein, and H. Schulzrinne, "MOSAIC: stateless mobility for HTTP-based applications," in *IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, (Barcelona, Spain), pp. 69–76, Oct. 2012.

[24] S. Srinivasan, A. Singh, D. Batni, J. W. Lee, H. Schulzrinne, V. Hilt, and G. Kunzmann, "CCNxServ: dynamic service scalability in Information-Centric networks," in *IEEE ICC 2012 - Next-Generation Networking Symposium (ICC'12 NGN)*, (Ottawa, Ontario, Canada), pp. 2632–2637, June 2012.

[25] E. Maccherani, M. Femminella, J. W. Lee, R. Francescangeli, J. Janak, G. Reali, and H. Schulzrinne, "Extending the netserv autonomic management capabilities using openflow," in *Network Operations and Management Symposium (NOMS), 2012 IEEE*, (Maui, Hawaii), pp. 582–585, Apr. 2012.

[26] M. Femminella, R. Francescangeli, G. Reali, and H. Schulzrinne, "Gossip-based signaling dissemination extension for next steps in signaling," in *Network Operations and Management Symposium (NOMS)*, (Maui, Hawaii), pp. 1022–1028, Apr. 2012.

[27] A. Moghadam, T. Jebara, and H. Schulzrinne, "A markov routing algorithm for mobile DTNs based on Spatio-Temporal modeling of human movement data," in *14th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM 2011)*, (Miami Beach, USA), Oct. 2011.

[28] M. Femminella, R. Francescangeli, G. Reali, J. W. Lee, W. Song, and H. Schulzrinne, "Future internet autonomic management using NetServ," in *Demonstrations of the IEEE Conference on Local Computer Networks (LCN) (LCN-Demos 2011)*, (Bonn, Germany), pp. 1081–1083, Oct. 2011.

[29] F. M. Roberto, J. Celestino JÃºnior, and H. Schulzrinne, "Using a symmetric game based in volunteer's dilemma to improve vanets multihop broadcast communication," in *22nd IEEE Personal Indoor Mobile Radio Communications (PIMRC'11 - ITN)*, (Toronto, Canada), pp. 777–782, Sept. 2011.

[30] J. Y. Kim, G. Bond, E. Cheung, T. M. Smith, and H. Schulzrinne, "An evaluation framework for highly available and scalable SIP server clusters," in *Principles, Systems and Applications of IP Telecommunications (IPTComm'11)*, (Chicago, Illinois, USA), Aug. 2011.

[31] K. Ono and H. Schulzrinne, "Using Cross-Media relations to identify important communication requests: Testing the concept and implementation," in *Principles, Systems and Applications of IP Telecommunications (IPTComm'11)*, (Chicago, Illinois, USA), Aug. 2011.

[32] J. Y. Kim and H. Schulzrinne, "SipCloud: dynamically scalable SIP proxies in the cloud," in *Principles, Systems and Applications of IP Telecommunications (IPTComm'11)*, (Chicago, Illinois, USA), Aug. 2011.

[33] O. Boyaci, V. Beltran, and H. Schulzrinne, "Bridging communications and the physical world: Sense everything, control everything," in *Principles, Systems and Applications of IP Telecommunications (IPTComm'11)*, (Chicago, Illinois, USA), Aug. 2011.

[34] E. Shim, V. Krishnaswamy, and H. Schulzrinne, "Automatic phone number mapping verification for phone number based SIP peering," in *The 8th Annual IEEE Consumer Communications and Networking Conference - Content Distribution and Peer-to-Peer Networks (CCNC'2011 Content Distribution and Peer-to-Peer Networks)*, (Las Vegas, NV, USA), pp. 995–999, Jan. 2011.

[35] S. Srinivasan, I. Rimac, M. Steiner, V. Hilt, and H. Schulzrinne, "Unveiling the content-centric features of TCP," in *ICC 2011 Next Generation Networking and Internet Symposium (ICC'11 NGNI)*, (Kyoto, Japan), June 2011.

[36] W. Song, J. W. Lee, and H. Schulzrinne, "Polygon simplification for Location-Based services using population density," in *ICC 2011 - Communication Software, Services and Multimedia Applications Symposium (ICC'11 CSMA)*, (Kyoto, Japan), June 2011.

[37] J. W. Lee, H. Schulzrinne, W. Kellerer, and Z. Despotovic, "0 to 10k in 20 seconds: Bootstrapping large-scale DHT networks," in *ICC 2011 - Communication Software, Services and Multimedia Applications Symposium (ICC'11 CSMA)*, (Kyoto, Japan), June 2011.

[38] J. W. Lee, R. Francescangeli, J. Janak, S. Srinivasan, S. A. Baset, H. Schulzrinne, Z. Despotovic, and W. Kellerer, "NetServ: active networking 2.0," in *ICC 2011 Workshop TF1 (T2), Future Network (ICC'11 Workshop TF1 (T2) FutureNet IV)*, (Kyoto, Japan), June 2011.

[39] S. Komorita, H. Yokota, A. Dutta, C. Makaya, S. Das, D. A. Chee, F. J. Lin, and H. Schulzrinne, "User-transparent reconfiguration method for self-organizing IP multimedia subsystem," in *16th IEEE Symposium on Computers and Communications (IEEE ISCC 2011)*, (Kerkyra (Corfu), Greece), June 2011.

[40] A. Dutta, B. Lyles, and H. Schulzrinne, "A formal approach to mobility modeling," in *The Third International Conference on COMmunication Systems and NETworkS (COMSNETS 2011) (COMSNETS 2011)*, (Bangalore, India), Jan. 2011.

[41] J. Kayfetz, H. Schulzrinne, T. Sherwood, and M. Tiwari, "Your desktop or mine: Extending the reach of writing instruction," in *Ubiquitous Learning International Conference ()*, (Vancouver, Canada), Dec. 2010.

[42] C. Makaya, A. Dutta, B. Falchuk, D. A. Chee, S. Das, F. J. Lin, M. Ito, S. Komorita, T. Chiba, H. Yokota, and H. Schulzrinne, "Enhanced Next-Generation service overlay networks architecture," in *IEEE International Conference on Internet Multimedia Systems Architecture and Application (IMSAA-10)*, (Bangalore, India), Dec. 2010.

[43] O. Boyaci, V. Beltran, and H. Schulzrinne, "Bridging communications and the physical world: Sense everything, control everything," in *IEEE Globecom 2010 Workshop on Ubiquitous Computing and Networks (UbiCoNet 2010)*, (Miami, Florida, USA), pp. 1735–1740, Dec. 2010.

[44] S. G. Hong, H. Schulzrinne, and S. Weiland, "Signaling architecture for network traffic authorization," in *IEEE Globecom 2010 - Communication & Information System Security (GC10 - CIS)*, (Miami, Florida, USA), Dec. 2010.

[45] C. Shen and H. Schulzrinne, "On TCP-based SIP server overload control," in *Principles, Systems and Applications of IP Telecommunications (IPTComm'10)*, (Munich, Germany), Aug. 2010.

[46] M. Barnes, L. Miniero, R. Presta, S. P. Romano, and H. Schulzrinne, "CCMP: a novel standard protocol for conference management in the XCON framework," in *Principles, Systems and Applications of IP Telecommunications (IPTComm'10)*, (Munich, Germany), Aug. 2010.

[47] S. A. Baset and H. Schulzrinne, "Reliability and relay selection in Peer-to-Peer communication systems," in *Principles, Systems and Applications of IP Telecommunications (IPTComm'10)*, (Munich, Germany), Aug. 2010.

[48] C. Shen, E. Nahum, H. Schulzrinne, and C. P. Wright, "The impact of TLS on SIP server performance," in *Principles, Systems and Applications of IP Telecommunications (IPTComm'10)*, (Munich, Germany), Aug. 2010.

[49] A. Amirante, S. P. Romano, H. Schulzrinne, and K. H. Kim, "Online Non-Intrusive diagnosis of One-Way RTP faults in VoIP networks using cooperation," in *Principles, Systems and Applications of IP Telecommunications (IPTComm'10)*, (Munich, Germany), Aug. 2010.

[50] K. Sung, S. Srinivasan, and H. Schulzrinne, "BBS-ONE: bulletin board and forum system for mobile opportunistic networks," in *IEEE WCNIS2010-Wireless Networks (IEEE WCNIS2010-WN)*, (Beijing, China, P.R. China), June 2010.

[51] K. Andersson, A. G. Forte, and H. Schulzrinne, "Enhanced mobility support for roaming users: Extending the IEEE 802.21 information service," in *8th International Conference on Wired / Wireless Internet Communications (WWIC 2010)*, (Lulea, Sweden), May 2010.

[52] A. Cooper, H. Schulzrinne, E. Wilde, and D. Mulligan, "Challenges for the Location-Aware web," in *WebSci10: Extending the Frontiers of Society On-Line ()*, (Raleigh, North Carolina), Apr. 2010.

[53] A. Misra and H. Schulzrinne, "Policy-Driven distributed and collaborative demand response in Multi-Domain commercial buildings," in *1st Int'l Conf. on Energy-Efficient Computing and Networking ()*, (Passau, Germany), Apr. 2010.

[54] K. Arabshian, C. Dickmann, and H. Schulzrinne, "Ontology-Based service discovery Front-End interface for GloServ," in *6th European Semantic Web Conference on The Semantic Web: Research and Applications*, (Heraklion, Crete, Greece), May 2009.

[55] W. Song, J. Y. Kim, H. Schulzrinne, P. Boni, and M. Armstrong, "Using IM and SMS for emergency text communications," in *Principles, Systems and Applications of IP Telecommunications*, (Atlanta, Georgia, USA), July 2009.

[56] K. Ono and H. Schulzrinne, "Have i met you before? using Cross-Media relations to reduce SPIT," in *Principles, Systems and Applications of IP Telecommunications*, (Atlanta, Georgia, USA), July 2009.

[57] H. Cui, S. Srinivasan, and H. Schulzrinne, "ONEChat: enabling group chat and messaging in opportunistic networks," in *HotMobile (Poster) ()*, (Annapolis, Maryland), Feb. 2010.

[58] M. Ge, S. Srinivasan, and H. Schulzrinne, "FileXChange: Drag-and-Drop file sharing in opportunistic networks," in *HotMobile (Poster) ()*, (Annapolis, Maryland), Feb. 2010.

[59] O. Boyaci, A. Forte, and H. Schulzrinne, "Performance of Video-Chat applications under congestion," in *Eleventh IEEE International Symposium on Multimedia*, (San Diego, California, USA), Dec. 2009.

[60] O. Boyaci, A. Forte, S. Baset, and H. Schulzrinne, "vdelay a tool to measure Capture-to-Display latency and frame-rate," in *Eleventh IEEE International Symposium on Multimedia*, (San Diego, California, USA), Dec. 2009.

[61] O. Boyaci, A. Forte, S. Baset, and H. Schulzrinne, "vdelay: A tool to measure Capture-to-Display latency and frame-rate," in *Eleventh IEEE International Symposium on Multimedia*, (San Diego, California, USA), Dec. 2009.

[62] A. Dutta, C. Makaya, S. Das, D. Chee, F. Lin, S. Komorita, T. Chiba, H. Yokota, and H. Schulzrinne, "Self organizing IP multimedia subsystem," in *IEEE International Conference on Internet Multimedia Systems Architecture and Application*, (Bangalore, India), Dec. 2009.

[63] S. Srinivasan, J. Lee, E. Liu, M. Kester, H. Schulzrinne, V. Hilt, S. Seetharaman, and A. Khan, "NetServ: dynamically deploying in-network services," in *2nd ACM Workshop on Re-Architecting the Internet*, (Rome, Italy), Dec. 2009.

[64] S. G. Hong, S. Srinivasan, and H. Schulzrinne, "Measurements of multicast service discovery in a campus wireless network," in *IEEE Globecom 2009 Communications Quality of Service, Reliability and Performance Modeling Symposium*, (Honolulu, Hawaii, USA), Nov. 2009.

[65] K. Yasukawa, A. Forte, and H. Schulzrinne, "Distributed delay estimation and call admission control in IEEE 802.11 wireless LANs," in *ICC 2009 Wireless Networking*, (Dresden, Germany, Germany), June 2009.

[66] A. Moghadam and H. Schulzrinne, "Interest-aware content distribution protocol for mobile disruption-tolerant networks," in *10th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, (Kos Island, Greece), June 2009.

[67] M. Tauil, A. Dutta, Y.-H. Cheng, S. Das, D. Baker, M. Yajnik, D. Famolari, Y. Ohba, and V. Fajardo, "Realization of IEEE 802.21 services and preauthentication framework," in *Testbeds and Research Infrastructures for the Development of Networks & Communities and Workshops*, Apr. 2009.

[68] S. Srinivasan, A. Moghadam, and H. Schulzrinne, "BonAHA: service discovery framework for mobile Ad-Hoc applications," in *2009 IEEE Consumer Communications and Networking Conference - Personal Ad Hoc and Sensor Networks*, (Las Vegas, USA), Jan. 2009.

[69] A. Dutta, B. Lyles, H. Schulzrinne, and J. Wang, "Systems modeling for IP-Based handoff using timed petri nets," in *42nd Hawaii International Conference on System Sciences*, (Big Island, Hawaii), Jan. 2009.

[70] J. Lee, H. Schulzrinne, W. Kellerer, and Z. Despotovic, "mDHT: multicast-augmented DHT architecture for high availability and immunity to churn," in *2009 IEEE Consumer Communications and Networking Conference - P2P and Content Delivery*, (Las Vegas, USA), Jan. 2009.

[71] V. Singh, H. Schulzrinne, and P. Boni, "A new SIP event package for group membership management in advanced communications," in *International Conference on Internet Multimedia Services Architecture and Applications*, (Bangalore, India), Dec. 2008.

[72] A. Dutta, F. Lin, S. Das, B. Lyles, T. Chiba, H. Yokota, H. Schulzrinne, and D. Chee, "A-IMS architecture analysis and experimental IPv6 testbed," in *The 1st International Conference on IP Multimedia Subsystems Architecture and Applications*, (Bangalore, India), Dec. 2008.

[73] O. Boyaci and H. Schulzrinne, "BASS application sharing system," in *Tenth IEEE International Symposium on Multimedia*, (Berkeley, California, USA), Dec. 2008.

[74] T. Okabe and H. Schulzrinne, "Peer-to-Peer SIP features to eliminate a SIP sign-up process," in *IEEE Globecom 2008 Communications Software and Services Symposium*, (New Orleans, LA, USA), Nov. 2008.

[75] K. Ono and H. Schulzrinne, "The impact of SCTP on server scalability and performance," in *IEEE Globecom 2008 Communications Quality of Sevice, Reliability, and Performance Modeling Symposium*, (New Orleans, LA, USA), Nov. 2008.

[76] A. Forte and H. Schulzrinne, "Deployment guidelines for highly congested IEEE 802.11b/g networks," in *LANMAN 2009*, (Chij-Napoca, Transylvania), Sept. 2008.

[77] A. Moghadam, S. Srinivasan, and H. Schulzrinne, "7DS - a modular platform to develop mobile disruption-tolerant applications," in *International Conference and Exhibition on Next Generation Mobile Applications, Services, and Technologies*, (Cardiff, Wales, United Kingdom), Sept. 2008.

[78] T. Chiba, H. Yokota, A. Dutta, D. Chee, and H. Schulzrinne, "Performance analysis of next generation mobility protocols for IMS/MMD networks," in *IWCMC 2008 Next Generation Mobile Networks Symposium*, (Chania Crete Island, Greece, Greece), Aug. 2008.

[79] C. Shen, H. Schulzrinne, and E. Nahum, "SIP server overload control: Design and evaluation," in *Principles, Systems and Applications of IP Telecommunications*, (Heidelberg, Germany), July 2008.

[80] A. Forte and H. Schulzrinne, "Template-based signaling compression for Push-To-Talk over cellular (PoC)," in *Principles, Systems and Applications of IP Telecommunications*, (Heidelberg, Germany), July 2008.

[81] G. Ormazabal, H. Schulzrinne, E. Yardeni, and S. Nagpal, "Secure SIP: a scalable prevention mechanism for DoS attacks on SIP based VoIP systems," in *Principles, Systems and Applications of IP Telecommunications*, (Heidelberg, Germany), July 2008.

[82] K. Ono and H. Schulzrinne, "One server per city: Using TCP for very large SIP servers," in *Principles, Systems and Applications of IP Telecommunications*, (Heidelberg, Germany), July 2008.

[83] S. Baset, E. Brosh, D. Rubenstein, and H. Schulzrinne, "The delay friendliness of TCP," in *SIGMETRICS 2008–International Conference on Measurement and Modeling of Computer Systems*, (Annapolis, Maryland, USA), June 2008.

[84] S. Greco Polito and H. Schulzrinne, "SIP and 802.21 for service mobility and proactive authentication," in *Sixth Annual Conference on Communication Networks and Services Research*, (Halifax, Nova Scotia, Canada), May 2008.

[85] V. Singh, H. Schulzrinne, and K. Miao, "DYSWIS: an architecture for automated diagnosis of networks," in *Network Operations and Management Symposium (NOMS)*, (Salvador, Bahia), Apr. 2008.

[86] W. Kho, S. Baset, and H. Schulzrinne, "Skype relay calls: Measurements and experiments," in *11th IEEE Global Internet Symposium 2008*, (Phoenix, AZ, USA), Apr. 2008.

[87] R. Dantu, H. Schulzrinne, and P. Sroufe, "Experiences in building a multi-university testbed for research in multimedia communications," in *IEEE International Conference on Parallel and Distributed (IPDPS)*, (Miami, Florida), Apr. 2008.

[88] K. Arabshian and H. Schulzrinne, "An ontology-based hierarchical Peer-to-Peer global service discovery system," *Journal of Ubiquitous Computing and Intelligence (JUCI)*, Vol. 1, pp. 133–144, Dec. 2007.

[89] S. G. Hong, S. Srinivasan, and H. Schulzrinne, "Accelerating service discovery in ad-hoc zero configuration networking," in *IEEE Globecom 2007 Ad-hoc and Sensor Networking Symposium*, (Washington, DC, USA), Nov. 2007.

[90] A. Dutta, S. Chakravarty, K. Taniuchi, V. Vfajardo, Y. Ohba, D. Famolari, and H. Schulzrinne, "An experimental study of location assisted proactive handover," in *IEEE Globecom 2007 Internet Protocol Symposium*, (Washington, DC, USA), Nov. 2007.

[91] K. Yasukawa, A. Forte, and H. Schulzrinne, "Distributed delay estimation and call admission control in IEEE 802.11 WLANs," in *15th IEEE International Conference on Network Protocols*, (Beijing, P.R. China), pp. 334–335, Oct. 2007.

[92] A. Dutta, B. Lyles, H. Schulzrinne, T. Chiba, H. Yokota, and A. Idoue, "Generalized modeling framework for handoff analysis," in *18th International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC)*, Sept. 2007.

[93] S. Gandhi, V. Singh, and H. Schulzrinne, "Analyzing user behavior in instant messaging," in *The First Annual Conference of ITA*, (Maryland, USA), Sept. 2007.

[94] R. Lopez, A. Dutta, Y. Ohba, H. Schulzrinne, and A. Skarmeta, "Network-Layer assisted mechanism to optimize authentication delay during handoff in 802.11 networks," in *MobiQuitous*, Aug. 2007.

[95] S. Greco Polito, H. Schulzrinne, and A. Forte, "Inter-provider AAA and billing of VoIP users with token-based method," in *Global Information Infrastructure Symposium*, July 2007.

[96] R. Shacham, H. Schulzrinne, W. Kellerer, and S. Thakolsri, "Composition for enhanced SIP presence," in *12th IEEE Symposium on Computers and Communications*, (Aveiro, Portugal), July 2007.

[97] C. Shen and H. Schulzrinne, "Measurement and evaluation of ENUM server performance," in *ICC 2007 Network Services and Operation Symposium*, (Glasgow, Scotland, United Kingdom), June 2007.

[98] S. Srinivasan, A. Moghadam, S. G. Hong, and H. Schulzrinne, "7DS - node cooperation and information exchange in mostly disconnected networks," in *ICC 2007 Wireless Adhoc and Sensor Networks Symposium*, (Glasgow, Scotland, United Kingdom), June 2007.

[99] S. Shin and H. Schulzrinne, "Experimental measurement of the capacity for VoIP traffic in IEEE 802.11 WLANs," in *IEEE INFOCOM 2007*, (Anchorage, Alaska, USA), May 2007.

[100] T. Chiba, H. Yokota, A. Idoue, A. Dutta, S. Das, F. Lin, and H. Schulzrinne, "Mobility management schemes for heterogeneity support in next generation wireless networks," in *3rd Euro-NGI Conference on Next Generation Internet Networks - Design and Engineering for Heterogeneity*, (Trondheim, Norway), May 2007.

[101] S. Greco Polito and H. Schulzrinne, "Authentication and authorization method in multi-domain, multi-provider networks," in *3rd Euro-NGI Conference on Next Generation Internet Networks - Design and Engineering for Heterogeneity*, (Trondheim, Norway), May 2007.

[102] T. Chiba, H. Yokota, A. Idoue, A. Dutta, K. Manousakis, S. Das, and H. Schulzrinne, "Trombone routing mitigation techniques for IMS/MMD networks," in *IEEE Wireless Communications and Networking Conference 2007 - Networking*, (Hong Kong, Hong Kong), Mar. 2007.

[103] V. Singh, H. Schulzrinne, P. Boni, B. Elman, and D. Kenneson, "Presence aware Location-Based service for managing mobile communications," in *2007 IEEE Consumer Communications and Networking Conference - Enabling Technologies Track*, (Las Vegas, NV, USA), Jan. 2007.

[104] W. Yuen and H. Schulzrinne, "Improving search efficiency using bloom filters in partially connected ad hoc networks: A Location-Centric analysis," in *IEEE Globecom 2006 - Wireless Ad Hoc and Sensor Networks - towards Anytime Anywhere Internetworking*, Nov. 2006.

[105] S. Shin, A. Forte, and H. Schulzrinne, "Passive duplicate address detection for the dynamic host configuration protocol (DHCP)," in *IEEE Globecom 2006 - Internet Services and Enabling Technologies*, Nov. 2006.

[106] S. Patnaik, E. Yardeni, H. Schulzrinne, G. Ormazabal, and D. Helms, "Securing SIP: scalable mechanisms for protecting SIP-Based VoIP systems," in *NANOG (North American Network Operators Group)*, (St. Louis, Missouri), NANOG, Oct. 2006.

[107] A. Forte, S. Shin, and H. Schulzrinne, "Improving layer 3 handoff delay in IEEE 802.11 wireless networks," in *Wireless Internet Conference (WICON)*, Aug. 2006.

[108] W. Yuen and H. Schulzrinne, "Performance evaluation of time-based and hop-based TTL schemes in partially connected ad hoc networks," in *ICC 2006 Wireless Ad Hoc and Sensor Networks*, June 2006.

[109] W. Zhao and H. Schulzrinne, "DotSlash: an automated web hotspot rescue system with on-demand query result caching," in *IEEE International Conference on Autonomic Computing (ICAC) (poster session)*, (Dublin, Ireland), June 2006.

[110] J. Y. Kim, W. Song, and H. Schulzrinne, "An enhanced VoIP emergency services prototype," in *Information Systems for Crisis Response and Management (ISCRAM)*, (Newark, New Jersey), ISCRAM, May 2006.

[111] A. Dutta, E. van den Berg, D. Famolari, V. Fajardo, Y. Ohba, K. Taniuchi, and H. Schulzrinne, "Dynamic buffering scheme for mobile handoff," in *PIMRC*, (Helsinki), IEEE, IEEE, 2006.

[112] A. Dutta, S. Das, D. Famolari, Y. Ohba, K. Taniuchi, V. Fajardo, T. Kodama, and H. Schulzrinne, "Secured seamless convergence across heterogeneous access networks," in *World Telecommunication Congress*, (Budapest), IEEE, IEEE, May 2006.

[113] X. Fu, H. Schulzrinne, H. Tschofenig, C. Dickmann, and D. Hogrefe, "Overhead and performance study of the general internet signaling transport (GIST) protocol," in *IEEE INFOCOM 2006*, (Barcelona, SPAIN), Apr. 2006.

[114] S. Baset and H. Schulzrinne, "An analysis of the skype Peer-to-Peer internet telephony protocol," in *IEEE INFOCOM 2006*, (Barcelona, SPAIN), Apr. 2006.

[115] A. Dutta, S. Madhani, W. Chen, O. Altintas, and H. Schulzrinne, "GPS assisted fast-handoff mechanism for real-time communication," in *2006 IEEE Sarnoff Symposium*, (Princeton NJ, USA), Mar. 2006.

[116] K. Singh and H. Schulzrinne, "Failover and load sharing in SIP telephony," in *International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)*, (Philadelphia, PA), July 2005.

[117] A. Dutta, B. Kim, T. Zhang, S. Baba, K. Taniuchi, Y. Ohba, and H. Schulzrinne, "Experimental analysis of multi interface mobility management with SIP and MIP," in *IEEE Wirelesscom*, IEEE, IEEE, June 2005.

[118] K. Singh and H. Schulzrinne, "Peer-to-Peer internet telephony using SIP," in *NOSSDAV 2005*, (Skamania, Washington), June 2005.

[119] A. Dutta, T. Zhang, S. Madhani, K. Taniuchi, K. Fujimoto, Y. Katsube, Y. Ohba, and H. Schulzrinne, "Secure universal mobility for wireless internet," *Mobile Computing and Communications Review (MC2R)*, 2005.

[120] A. Dutta, T. Zhang, Y. Ohba, K. Taniuchi, and H. Schulzrinne, "MPA assisted proactive handoff scheme," in *ACM Mobiquitous*, SIGMOBILE, ACM, 2005.

[121] A. Dutta, J. Burns, R. Jain, K. Wong, K. Young, and H. Schulzrinne, "Implementation and performance evaluation of application layer MIP-LR," in *IEEE Wirelesscom*, IEEE, IEEE, 2005.

[122] R. Shacham, H. Schulzrinne, S. Thakolsri, and W. Kellerer, "The virtual device: Expanding wireless communication services through service discovery and session mobility," in *IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, (Montreal, Canada), IEEE, Aug. 2005.

[123] X. Wu and H. Schulzrinne, "Handling feature interactions in the language for end system services," in *International Conference on Feature Interactions in Telecommunications and Software Systems (ICFI)*, June 2005.

[124] X. Wu and H. Schulzrinne, "Service learning in internet telephony," in *ICC 2005 Next Generation Networks for Universal Services*, (Seoul, Korea), May 2005.

[125] T. Kawata, S. Shin, A. Forte, and H. Schulzrinne, "Using dynamic PCF to improve the capacity for VoIP traffic in IEEE 802.11 networks," in *IEEE WCNC*, IEEE, Mar. 2005.

[126] J. Varghese-Chennikara, A. Dutta, A. Cheng, M. Elaoud, A. McAuley, I. Sebuktekin, D. Wong, H. Schulzrinne, and K. Young, "Integrated technologies for a survivable network," in *IEEE Wireless and Communications and Networking Conference*, (New Orleans, LA, USA), IEEE, IEEE, Mar. 2005.

[127] X. Wu and H. Schulzrinne, "Location-based services in internet telephony systems," in *IEEE Consumer Communications and Networking Conference*, (Las Vegas, Nevada), Jan. 2005.

[128] X. Wu and H. Schulzrinne, "sipc, a multi-function SIP user agent," in *7th IFIP/IEEE International Conference, Management of Multimedia Networks and Services (MMNS)*, pp. 269–281, IFIP/IEEE, Springer, Oct. 2004.

[129] A. Dutta, S. Madhani, W. Chen, O. Altintas, and H. Schulzrinne, "Fast-handoff schemes for application layer mobility management,," in *IEEE PIMRC*, IEEE, IEEE, Sept. 2004.

[130] K. Arabshian and H. Schulzrinne, "GloServ: global service discovery architecture," in *First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (Mobiquitous)*, Aug. 2004.

[131] W. Zhao and H. Schulzrinne, "Building an adaptive distributed web server system on the fly for handling web hotspots," in *ACM Symposium on Principles of Distributed Computing (PODC)*, (St. John's, Newfoundland, Canada), ACM, ACM, July 2004.

[132] B.-T. Wang and H. Schulzrinne, "A Denial-of-Service-Resistant IP traceback approach," in *The Ninth IEEE Symposium on Computers and Communications*, (Alexandria, Egypt), June 2004.

[133] B.-T. Wang and H. Schulzrinne, "A robust packet filtering method for high bandwidth aggregates," in *IEEE Canadian Conference on Electrical and Computer Engineering 2004*, (Niagara Falls, Ontario, Canada), May 2004.

[134] B.-T. Wang and H. Schulzrinne, "An IP traceback mechanism for reflective DoS attacks," in *IEEE Canadian Conference on Electrical and Computer Engineering 2004*, (Niagara Falls, Ontario, Canada), May 2004.

[135] A. Dutta, P. Agrawal, S. Das, M. Elaoud, D. Famolari, S. Madhani, A. McAuley, and B. Kim, "Realizing mobile wireless internet telephony and streaming multimedia testbed," *Computer Communications*, Vol. 27, pp. 725–738, May 2004.

[136] L. Amini, A. Shaikh, and H. Schulzrinne, "Effective peering for multi-provider content delivery services," in *IEEE Infocom 2004*, (Hong Kong), Mar. 2004.

[137] B.-T. Wang and H. Schulzrinne, "Multifunctional ICMP messages for e-services," in *IEEE International Conference on e-Technology, e-Commerce and e-Service*, (Grand Hotel, Taipei, Taiwan), pp. 355–363, IEEE, IEEE, Mar. 2004.

[138] A. Dutta, S. Das, P. Li, A. McAuley, Y. Ohba, S. Baba, and H. Schulzrinne, "Secured mobile multimedia communication for wireless internet," in *International Conference on Network Sensing and Control*, (Taipei, Taiwan), IEEE, IEEE, Mar. 2004.

[139] K. Singh, X. Wu, J. Lennox, and H. Schulzrinne, "Comprehensive multi-platform collaboration," in *Multimedia Computing and Networking*, (San Jose, California, USA), SPIE's 16th Annual Symposium, IS&T - The Society for Imaging Science and Technology, and SPIE - The International Society for Optical Engineering, Jan. 2004.

[140] B.-T. Wang and H. Schulzrinne, "Tracing high bandwidth aggregates," in *IASTED International Conference on Communication, Network, and Information Security (CNIS)*, (New York City, NY, USA), pp. 165–170, IASTED, ACTA Press, Dec. 2003.

[141] B.-T. Wang and H. Schulzrinne, "Analysis of denial-of-service attacks on denial-of-service defensive measures," in *Globecom 2003 - General Conference*, (San Francisco Marriott, CA), pp. 1339–1343, IEEE, IEEE, Dec. 2003.

[142] B.-T. Wang and H. Schulzrinne, "Detecting offensive routers: A straightforward approach," in *IEEE International Carnahan Conference on Security Technology (ICCST)*, (Grand Hotel, Taipei, Taiwan), pp. 460–467, IEEE, IEEE, Oct. 2003.

[143] D. Wong, A. Dutta, H. Schulzrinne, and K. Young, "Managing simultaneous mobility of IP hosts," in *IEEE International Military Communications Conference (MILCOM)*, (Boston, MA, USA), IEEE, IEEE, Oct. 2003.

[144] X. Fu, H. Schulzrinne, and H. Tschofenig, "Mobility support for next-generation internet signaling protocols," in *VTC 2003 - IP Mobility*, Oct. 2003.

[145] S. Berger, H. Schulzrinne, S. Sidiroglou, and X. Wu, "Ubiquitous computing using SIP," in *ACM NOSSDAV 2003*, (Monterey, California, USC), pp. 82–89, June 2003.

[146] X. Wu and H. Schulzrinne, "Programmable end system services using SIP," in *International Conference on Communications*, (Anchorage, Alaska), pp. 789–793, May 2003.

[147] W. Jiang, K. Koguchi, and H. Schulzrinne, "Qos evaluation of voip end-points," in *ICC 2003 - Communication QoS, Reliability, and Performance Modeling*, May 2003.

[148] J. Lennox and H. Schulzrinne, "A protocol for reliable decentralized conferencing," in *ACM NOSSDAV 2003*, (Monterey, California, USC), June 2003.

[149] W. Zhao and H. Schulzrinne, "Predicting the upper bound of web traffic volume using a multiple time scale approach," in *International World Wide Web Conference (WWW) (poster session)*, (Budapest, Hungary), p. 243, May 2003.

[150] P.-Y. Hsieh, A. Dutta, and H. Schulzrinne, "Application layer mobility proxy for real-time communication," in *World Wireless Congress, 3G Wireless*, (San Francisco), Delson, Delson, May 2003.

[151] K. Singh, A. Nambi, and H. Schulzrinne, "Integrating voicexml with SIP services.," in *ICC 2003 - Global Services and Infrastructure for Next Generation Networks*, (Anchorage, Alaska), May 2003.

[152] L. Amini and H. Schulzrinne, "Modeling redirection in geographically diverse server sets," in *WWW*, (Budapest, Hungary), May 2003.

[153] N. Nakajima, A. Dutta, S. Das, and H. Schulzrinne, "Handoff delay analysis and measurement for SIP based mobility in ipv6," in *ICC 2003 - Personal Communication Systems and Wireless LANs*, May 2003.

[154] P. Mendes, H. Schulzrinne, and E. Monteiro, "Signaling protocol for session-aware popularity-based resource allocation," in *IFIP/IEEE International Conference on Management of Multimedia Networks and Services*, University of Santa Barbara, Oct. 2002.

[155] A. Dutta, D. Wong, J. Burns, R. Jain, K. Young, A. McAuley, and H. Schulzrinne, "Realization of integrated mobility management for ad-hoc networks," in *IEEE Milcom*, (Annaheim, California), Oct. 2002.

[156] L. Amini and H. Schulzrinne, "On probe strategies for dynamic multimedia server selection," in *IEEE Conference on Multimedia and Expo*, IEEE, Aug. 2002.

[157] L. Amini, A. Shaikh, and H. Schulzrinne, "Issues with inferring Internet topological attributes," in *ITcom Internet Performance and Control of Network Systems*, SPIE, July 2002.

[158] H. Schulzrinne and K. Arabshian, "Emergency calls and notifications," in *ITCom*, (Boston, Massachusetts), July/August 2002.

[159] W. Zhao and H. Schulzrinne, "Selective anti-entropy," in *ACM Symposium on Principles of Distributed Computing (PODC)*, (Monterey, California), ACM, ACM, July 2002.

[160] A. Dutta, O. Altintas, W. Chen, and H. Schulzrinne, "Mobility approaches for all IP wireless networks," in *SCI*, (Orlando, Florida), July 2002.

[161] P. Koskelainen, H. Schulzrinne, and X. Wu, "A SIP-based conference control framework," in *Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV)*, (Miami Beach, Florida), pp. 53–61, May 2002.

[162] W. Jiang and H. Schulzrinne, "Speech recognition performance as an effective perceived quality predictor," in *IWQoS*, (Miami Beach), May 2002.

[163] P. Mendes, H. Schulzrinne, and E. Monteiro, "Session-aware popularity resource allocation for assured differentiated services," in *Networking*, (Pisa, Italy), May 2002.

[164] W. Jiang and H. Schulzrinne, "Comparison and optimization of packet loss repair methods on VoIP perceived quality under bursty loss," in *Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV)*, (Miami Beach, Florida), May 2002.

[165] A. Dutta, J. Chen, S. Madhani, A. McAuley, N. Nakajima, and H. Schulzrinne, "Implementing a testbed for mobile multimedia," in *Proceedings of the IEEE Conference on Global Communications (GLOBECOM)*, (San Antonio, Texas), Nov. 2001.

[166] A. Dutta, R. Jain, D. Wong, J. Burns, K. Young, and H. Schulzrinne, "Multilayered mobility management for survivable network," in *Milcom*, (Vienna, Virginia), Nov. 2001.

[167] M. Papadopouli and H. Schulzrinne, "Effects of power conservation, wireless coverage and cooperation on data dissemination among mobile devices," in *Mobihoc*, (Long Beach, California), Oct. 2001.

[168] K. Wong, H.-Y. Wei, A. Dutta, K. Young, and H. Schulzrinne, "Performance of IP micro-mobility management scheme using host based routing," in *WPMC*, (Denmark), Aug. 2001.

[169] P. Pan and H. Schulzrinne, "Processing overhead studies in resource reservation protocols," in *17th International Teletraffic Congress*, (Salvador da Bahia, Brazil), Sept. 2001.

[170] H. Schulzrinne, "Keynote: Quality of service - 20 years old and ready to get a job?," *Lecture Notes in Computer Science*, Vol. 2092, p. 1, June 2001. International Workshop on Quality of Service (IWQoS).

[171] A. Dutta and H. Schulzrinne, "A streaming architecture for next generation Internet," in *Conference Record of the International Conference on Communications (ICC)*, (Helsinki), p. 7, June 2001.

[172] A. Dutta, F. Vakil, J. Chen, M. Tauil, S. Baba, and H. Schulzrinne, "Application layer mobility management scheme for wireless Internet," in *3Gwireless*, (San Francisco), p. 7, May 2001.

[173] A. Dutta, H. Schulzrinne, W. Chen, and O. Altintas, "Mobility support for wireless streaming multimedia in marconinet," in *IEEE Broadband Wireless Summit, Interop*, (Las Vegas), p. 7, May 2001.

[174] J. Brassil and H. Schulzrinne, "Enhancing Internet streaming media with cueing protocols," in *Proceedings of the Conference on Computer Communications (IEEE Infocom)*, (Anchorage, Alaska), Apr. 2001.

[175] X. Wang and H. Schulzrinne, "Pricing network resources for adaptive applications in a differentiated services network," in *Proceedings of the Conference on Computer Communications (IEEE Infocom)*, (Anchorage, Alaska), Apr. 2001.

[176] W. Zhao, H. Schulzrinne, and E. Guttman, "mSLP - mesh-enhanced service location protocol," in *International Conference on Computer Communication and Network*, (Las Vegas, Nevada), Oct. 2000.

[177] X. Wang, C. Yu, H. Schulzrinne, P. Stirpe, and W. Wu, "IP multicast faulty recovery in PIM over OSPF," in *International Conference on Network Protocols (ICNP)*, (Osaka, Japan), Nov. 2000.

[178] M. Papadopouli and H. Schulzrinne, "Seven degrees of separation in mobile ad hoc networks," in *Proceedings of the IEEE Conference on Global Communications (GLOBECOM)*, (San Francisco, California), Nov. 2000.

[179] W. Jiang and H. Schulzrinne, "Analysis of on-off patterns in VoIP and their effect on voice traffic aggregation," in *International Conference on Computer Communication and Network*, (Las Vegas, Nevada), Oct. 2000.

[180] M. Papadopouli, H. Schulzrinne, P. Castro, P. Kermani, C. Bisdikian, and M. Naghshineh, "Data gathering and distribution across widely distributed devices," in *SIGCOMM Symposium on Communications Architectures and Protocols*, (Stockholm, Sweden), August/September 2000. student poster session.

[181] X. Wang and H. Schulzrinne, "Adaptive reservation: A new framework for multimedia adaptation," in *IEEE International Conference on Multimedia and Expo (ICME)*, (New York), July/August 2000.

[182] D. Sisalem and H. Schulzrinne, "The adaptive load service: An ABR-Like service for the Internet," in *5th IEEE Symposium on Computers and Communications (ISCC)*, (Juan Les Pins, France), July 2000.

[183] X. Wang, C.-M. Yu, H. Schulzrinne, P. Stirpe, and W. Wu, "IP multicast fault recovery in PIM over OSPF," in *Proceedings of the ACM Sigmetrics Conference on Measurement and Modeling of Computer Systems*, (Santa Clara, California), June 2000.

[184] X. Wang, H. Schulzrinne, D. Kandlur, and D. Verma, "Measurement and analysis of LDAP performance," in *Proceedings of the ACM Sigmetrics Conference on Measurement and Modeling of Computer Systems*, (Santa Clara, California), June 2000.

[185] J. Lennox and H. Schulzrinne, "Feature interaction in Internet telephony," in *Feature Interaction in Telecommunications and Software Systems VI*, (Glasgow, United Kingdom), May 2000.

[186] J. Rosenberg, L. Qiu, and H. Schulzrinne, "Integrating packet FEC into adaptive voice playout buffer algorithms on the Internet," in *Proceedings of the Conference on Computer Communications (IEEE Infocom)*, (Tel Aviv, Israel), Mar. 2000.

[187] E. Wedlund and H. Schulzrinne, "Mobility support using SIP," in *2nd ACM/IEEE International Conference on Wireless and Mobile Multimedia (WoWMoM)*, (Seattle, Washington), Aug. 1999.

[188] A. Dutta and H. Schulzrinne, "Marconinet - an architecture for Internet radio and TV networks," in *Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV)*, (Basking Ridge, New Jersey), pp. 241–245, June 1999.

[189] M. Papadopouli and H. Schulzrinne, "Connection sharing in an ad hoc wireless network among collaborating hosts," in *Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV)*, (Basking Ridge, New Jersey), pp. 169–185, June 1999.

[190] X. Wang and H. Schulzrinne, "RNAP: a resource negotiation and pricing protocol," in *Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV)*, (Basking Ridge, New Jersey), pp. 77–93, June 1999.

[191] H. Schulzrinne and J. Rosenberg, "Signaling for Internet telephony," in *International Conference on Network Protocols (ICNP)*, (Austin, Texas), Oct. 1998.

[192] P. Pan and H. Schulzrinne, "YESSIR: a simple reservation mechanism for the Internet," in *Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV)*, (Cambridge, England), pp. 141–151, July 1998. also IBM Research Technical Report TC20967.

[193] H. Schulzrinne and J. Rosenberg, "A comparison of SIP and H.323 for Internet telephony," in *Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV)*, (Cambridge, England), pp. 83–86, July 1998.

[194] D. Sisalem and H. Schulzrinne, "The loss-delay adjustment algorithm: A TCP-friendly adaptation scheme," in *Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV)*, (Cambridge, England), pp. 215–226, July 1998.

[195] I. Schubert, D. Sisalem, and H. Schulzrinne, "A session floor control scheme," in *International Conference on Telecommunications*, (Chalkidiki, Greece), June 1998.

[196] D. Sisalem, F. Emanuel, and H. Schulzrinne, "The direct adjustment algorithm: A TCP-Friendly adaptation scheme," 1998. submitted for publication.

[197] J. Rosenberg and H. Schulzrinne, "Internet telephony gateway location," in *Proceedings of the Conference on Computer Communications (IEEE Infocom)*, (San Francisco, California), pp. 488–496, March/April 1998.

[198] J. Rosenberg and H. Schulzrinne, "Timer reconsideration for enhanced RTP scalability," in *Proceedings of the Conference on Computer Communications (IEEE Infocom)*, (San Francisco, California), March/April 1998.

[199] P. Pan and H. Schulzrinne, "Staged refresh timers for RSVP," in *Proceedings of Global Internet*, (Phoenix, Arizona), Nov. 1997. also IBM Research Technical Report TC20966.

[200] H. Schulzrinne, "A comprehensive multimedia control architecture for the Internet," in *Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV)*, (St. Louis, Missouri), May 1997.

[201] H. Schulzrinne, "Re-engineering the telephone system," in *IEEE Singapore International Conference on Networks (SICON)*, (Singapore), Apr. 1997.

[202] H. Schulzrinne, "Signaling for Internet telephony services," in *Opensig*, (New York, New York), Oct. 1996.

[203] H. Schulzrinne, "The impact of resource reservation for real-time Internet services," in *National Research Council (NRC) Workshop on Information System Trustworthiness*, (Washington, D.C.), Oct. 1996.

[204] D. Sisalem and H. Schulzrinne, "Congestion control in TCP: performance of binary congestion notification enhanced TCP compared to reno and tahoe TCP," in *International Conference on Network Protocols (ICNP)*, (Columbus, Ohio), pp. 268–275, Oct. 1996.

[205] D. Sisalem, H. Schulzrinne, and C. Sieckmeyer, "The network video terminal," in *HPDC Focus Workshop on Multimedia and Collaborative Environments (Fifth IEEE International Symposium on High Performance Distributed Computing)*, (Syracuse, New York), IEEE Computer Society, Aug. 1996.

[206] H. Schulzrinne, "The world-wide web as the universal interface to the NII," national research council (nrc) background paper, Columbia University, July 1996.

[207] D. Sisalem and H. Schulzrinne, "Binary congestion notification in TCP," in *Conference Record of the International Conference on Communications (ICC)*, (Dallas, Texas), IEEE, June 1996.

[208] D. Sisalem and H. Schulzrinne, "Switch mechanisms for the ABR service: A comparison study," in *Telecommunication Distribution Parallelism (TDP)*, (La Londes Les Maures, France), Institut National des Telecommunications, Evry, June 1996.

[209] H. Schulzrinne, M. Smirnov, R. Roth, and A. M. Wolisz, "IP multicasting over ATM: the multicube approach," in *3rd International Symposium on Interworking - INTERWORKING: High-Speed Networking and Interoperability*, (Nara, Japan), pp. 181–190, IOS Press/Ohmsha, Oct. 1996.

[210] H. Schulzrinne, "Personal mobility for multimedia services in the Internet," in *European Workshop on Interactive Distributed Multimedia Systems and Services (IDMS)*, (Berlin, Germany), Mar. 1996.

[211] D. Sisalem and H. Schulzrinne, "End-to-end rate control in ABR," in *1st Workshop on ATM Traffic Management (WATM)*, (Paris, France), pp. 281–287, IFIP WG 6.2, Dec. 1995.

[212] H. Schulzrinne, "When can we unplug the phone and the radio?," in *Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV)*, Lecture Notes in Computer Science (LNCS), (Durham, New Hampshire), pp. 183–184, Springer, Apr. 1995.

[213] H. Schulzrinne, "Internet services: from electronic mail to real-time multimedia," in *KIVS (Kommunikation in Verteilten Systemen)* (K. Franke, U. Hübner, and W. Kalfa, eds.), Informatik aktuell, (Chemnitz, Germany), pp. 21–34, Gesellschaft für Informatik, Springer Verlag, Feb. 1995.

[214] H. Schulzrinne, "Audio and video over packet networks — issues, architecture and protocols," in *INTEROP*, (Paris, France), Oct. 1994.

[215] H. Schulzrinne, "Conferencing and collaborative computing," in *Dagstuhl Seminar on Fundamentals and Perspectives of Multimedia Systems*, (Dagstuhl Castle, Germany), July 1994.

[216] H. Schulzrinne, J. F. Kurose, and D. F. Towsley, "An evaluation of scheduling mechanisms for providing best-effort, real-time communication in wide-area networks," in *Proceedings of the Conference on Computer Communications (IEEE Infocom)*, (Toronto, Canada), June 1994.

[217] R. Ramjee, J. F. Kurose, D. F. Towsley, and H. Schulzrinne, "Adaptive playout mechanisms for packetized audio applications in wide-area networks," in *Proceedings of the Conference on Computer Communications (IEEE Infocom)*, (Toronto, Canada), pp. 680–688, IEEE Computer Society Press, Los Alamitos, California, June 1994.

[218] H. Schulzrinne, J. F. Kurose, and D. F. Towsley, "Loss correlation for queues with bursty input streams," in *Conference Record of the International Conference on Communications (ICC)*, Vol. 1, (Chicago, Illinois), pp. 0219–0224 (308.4), IEEE, June 1992.

[219] H. Schulzrinne and J. F. Kurose, "Distribution of the loss period for some queues in continuous and discrete time," in *Proceedings of the Conference on Computer Communications (IEEE Infocom)*, (Bal Harbour, Florida), pp. 1446–1455 (12C.1), Apr. 1991.

[220] H. Schulzrinne, J. F. Kurose, and D. F. Towsley, "Congestion control for real-time traffic in high-speed networks," in *Proceedings of the Conference on Computer Communications (IEEE Infocom)*, Vol. 2, (San Francisco, California), pp. 543–550, June 1990.

[221] H. Schulz-Rinne, "The DSP workbench: Modeling parallel architectures as concurrent processes," in *IEEE International Conference on Acoustics, Speech, and Signal Processing 1986*, (Tokyo, Japan), pp. 54.9.1–54.9.4, IEEE, Apr. 1986.

WORKSHOPS

[1] A. Y. Ding, Y. Liu, S. Tarkoma, H. Flinck, H. Schulzrinne, and J. Crowcroft, "Vision: Augmenting wifi offloading with an open-source collaborative platform," in *Proceedings of the 6th International Workshop on Mobile Cloud Computing and Services*, (Paris, France), pp. 44–48, Sept. 2015.

[2] H. Schulzrinne, K.-H. Kim, H. Nam, V. Singh, and D. Song, "QoE: A micro and macro perspective," in *NSF/FCC workshop on Tracking Quality of Experience in the Internet*, (Princeton, New Jersey), Oct. 2015.

[3] A. Y. Ding, J. Korhonen, T. Savolainen, Y. Liu, M. Kojo, S. Tarkoma, and H. Schulzrinne, "Reflections on middlebox detection mechanisms in IPv6 transition," in *Internet Architecture Board Workshop on Stack Evolution in a Middlebox Internet (IAB SEMI)*, (Zurich, Switzerland), Jan. 2015.

[4] H. Schulzrinne, "The Internet is a series of tubes," in *Towards an Affordable Internet Access for Everyone: The Quest for Enabling Universal Service Commitment (Dagstuhl Seminar 14471)* (J. Crowcroft, A. Wolisz, and A. Sathiaseelan, eds.), no. 11 in Dagstuhl Reports, pp. 78–137, Dagstuhl, Germany: Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2015.

[5] A. Mehta, A. Forte, and H. Schulzrinne, "Using conference servers for SIP-based vertical handoff between IP and cellular networks," in *The 6th ACM International Workshop on Mobility Management and Wireless Access*, (Vancouver, British Columbia, Canada), Oct. 2008.

[6] S. Shin and H. Schulzrinne, "Call admission control in IEEE 802.11 WLANs using QP-CAT," in *The 27th IEEE International Conference on Computer Communications*, (Phoenix, Arizona, USA), Apr. 2008.

[7] J. Lee, H. Schulzrinne, W. Kellerer, and Z. Despotovic, "z2z: Discovering zeroconf services beyond local link," in *Globecom Workshops*, Nov. 2007.

[8] S. Srinivasan and H. Schulzrinne, "BonSwing: a GUI framework for Ad-Hoc applications using service discovery," in *CoNEXT Student Workshop*, (New York, USA), Dec. 2007.

[9] J. Lee, H. Schulzrinne, W. Kellerer, and Z. Despotovic, "Bootstrapping large-scale DHT networks," in *CoNEXT Student Workshop*, (New York, USA), Dec. 2007.

[10] O. Boyaci and H. Schulzrinne, "Application and desktop sharing," in *CoNEXT Student Workshop*, (New York, USA), Dec. 2007.

[11] V. Janardhan and H. Schulzrinne, "Peer assisted VoD for set-top box based IP network," in *P2P-TV '07: the 2007 workshop on Peer-to-peer streaming and IP-TV*, (Kyoto, Japan), Aug. 2007.

[12] H. Schulzrinne, H. Tschofenig, A. Newton, and T. Hardie, "LoST: a protocol for mapping geographic locations to public safety answering points," in *The First International Workshop on Next Generation Networks for First Responders and Critical Infrastructure*, (New Orleans, Louisiana, USA), Apr. 2007.

[13] H. Tschofenig, H. Schulzrinne, A. Newton, and M. Shanmugam, "Protecting First-Level responder resources in an IP-based emergency services architecture," in *The First International Workshop on Next Generation Networks for First Responders and Critical Infrastructure*, (New Orleans, Louisiana, USA), Apr. 2007.

[14] W. Yuen and H. Schulzrinne, "Localization for intermittently connected ad hoc networks," in *International Workshop on Intermittently Connected Mobile Ad Hoc Networks*, (Hoes Lane, Piscataway, NJ 08854), IEEE, IEEE, Mar. 2007.

[15] H. Schulzrinne, A. Forte, and S. Shin, "User mobility in IEEE 802.11 networks," in *Proceedings of first ACM/IEEE international workshop on Mobility in the evolving internet architecture*, (San Francisco, California), pp. 7–8, ACM, Dec. 2006.

[16] M. Cristofano, A. Forte, H. Schulzrinne, and M. Longo, "A generic model for mobility management in beyond third generation networks," in *The First International Workshop on Broadband and Wireless Computing, Communication and Applications*, (Yogyakarta, Indonesia), IIWAS, Dec. 2006.

[17] S. Patnaik, E. Yardeni, H. Schulzrinne, G. Ormazabal, and D. Helms, "Securing SIP: scalable mechanisms for protecting SIP-Based VoIP systems," in *NANOG (North American Network Operators Group)*, (St. Louis, Missouri), NANOG, Oct. 2006.

[18] H. Tschofenig, H. Schulzrinne, and A. Newton, "IETF mapping protocol architecture," in *First SDO Emergency Services Coordination Workshop*, (New York, NY, USA), Oct. 2006.

[19] H. Schulzrinne, J. Polk, M. Linsner, and A. Newton, "IETF GEOPRIV: transmission of location information using DHCP," in *First SDO Emergency Services Coordination Workshop*, (New York, NY, USA), Oct. 2006.

[20] H. Schulzrinne and H. Tschofenig, "Emergency service identification," in *First SDO Emergency Services Coordination Workshop*, (New York, NY, USA), Oct. 2006.

[21] H. Tschofenig, H. Schulzrinne, A. Newton, J. Peterson, and A. Mankin, "The IETF geopriv and presence architecture focusing on location privacy," in *W3C Workshop on Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement*, (Ispra, Italy), W3C, Oct. 2006.

[22] H. Tschofenig, H. Schulzrinne, M. Linsner, J. Polk, and B. Rosen, "IETF ECRIT emergency service architecture," in *First SDO Emergency Services Coordination Workshop*, (New York, NY, USA), Oct. 2006.

[23] A. Forte, S. Shin, and H. Schulzrinne, "Improving layer 3 handoff delay in IEEE 802.11 wireless networks," in *Wireless Internet Conference (WICON)*, Aug. 2006.

[24] S. Shin and H. Schulzrinne, "Balancing uplink and downlink delay of VoIP trafc in WLANs using adaptive priority control (APC)," in *Qshine (3rd international conference on Quality of service in heterogeneous wired/wireless networks)*, Aug. 2006.

[25] K. Arabshian and H. Schulzrinne, "Distributed context-aware agent architecture for global service discovery," in *The Second International Workshop on Semantic Web Technology For Ubiquitous and Mobile Applications (SWUMA '06)*, 2006.

[26] K. Arabshian, H. Schulzrinne, D. Trossen, and D. Pavel, "GloServ: global service discovery using the OWL web ontology language," in *IEE International Workshop on Intelligent Environments (IE05)*, IEE, June 2005.

[27] C. Shen, H. Schulzrinne, S.-H. Lee, and J. Bang, "Routing dynamics measurement and detection for next step internet signaling protocol," in *IEEE/IFIP Workshop on End-to-End Monitoring Techniques and Services (E2EMON)*, IEEE/IFIP, May 2005.

[28] X. Wu, R. Shacham, M. Mintz-Habib, K. Singh, and H. Schulzrinne, "Location-based communication services," in *International Multimedia Conference, Workshop on Effective Telepresence*, pp. 55–56, ACM, Oct. 2004.

[29] A. Dutta, T. Zhang, S. Madhani, K. Taniuchi, K. Fujimoto, H. Schulzrinne, Y. Ohba, and Y. Katsube, "Secure universal mobility for wireless internet," in *The Second ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots*, (Philadelphia, PA,), Oct. 2004.

[30] W. Zhao and H. Schulzrinne, "DotSlash: a self-configuring and scalable rescue system for handling web hotspots effectively," in *International Workshop on Web Caching and Content Distribution (WCW)*, (Beijing, China), Oct. 2004.

[31] S. Shin, H. Schulzrinne, A. Forte, and A. Rawat, "Reducing MAC layer handoff latency in IEEE 802.11 wireless LANs," in *ACM MobiWac (ACM International Workshop on Mobility Management and Wireless Access)*, (Philadelphia, Pennsylvania), ACM, Sept. 2004.

[32] C. Wieser, M. Laakso, and H. Schulzrinne, "SIP robustness testing for Large-Scale use," in *First International Workshop on Software Quality (SOQA)*, (Erfurt, Germany), Sept. 2004.

[33] K. Arabshian and H. Schulzrinne, "Glo-Serv: global service discovery architecture," in *MobiQuitous 2004 Services*, (Boston, Massachusetts, USA), Aug. 2004.

[34] R. Shacham, H. Schulzrinne, W. Kellerer, and S. Thakolsri, "An architecture for location-based service mobility using the SIP event model," in *ACM International Conference on Mobile Systems, Applications and Services (MobiSys), Workshop on Context Awareness*, ACM, June 2004.

[35] S. Khurana, A. Dutta, P. Gurung, and H. Schulzrinne, "XML based wide area communication with networked appliances," in *2004 IEEE Sarnoff Symposium*, (Princeton, New Jersey), Apr. 2004.

[36] K. Arabshian and H. Schulzrinne, "A generic event notification system using XML and SIP," in *New York Metro Area Networking Workshop 2003*, (Bern Dibner Library Building, LC400, Polytechnic University, 5 Metrotech Cente), Sept. 2003.

[37] B.-T. Wang and H. Schulzrinne, "A denial-of-service-resistant IP traceback approach," in *New York Metro Area Networking Workshop 2003*, (Bern Dibner Library Building, LC400, Polytechnic University, 5 Metrotech Cente), Sept. 2003.

[38] W. Jiang and H. Schulzrinne, "A black-box qos measurement methodology for voip end-points," in *New York Metro Area Networking Workshop 2003*, (Bern Dibner Library Building, LC400, Polytechnic University, 5 Metrotech Cente), Sept. 2003.

[39] K. Arabshian and H. Schulzrinne, "A sip-based medical event monitoring system," in *5th International Workshop on Enterprise Networking and Computing in Healthcare Industry (HealthCom)*, (Santa Monica, CA), June 2003.

[40] W. Jiang and H. Schulzrinne, "Assessment of voip service availability in the current internet," in *Passive & Active Measurement Workshop*, (San Diego, CA), Apr. 2003.

[41] P. Mendes, H. Schulzrinne, and E. Monteiro, "A receiver-driven adaptive mechanism based on the popularity of scalable sessions," in *COST 263 International Workshop on Quality of future Internet Services (QofIS)*, ETH Zurich, Oct. 2002.

[42] A. Dutta, H. Schulzrinne, O. Altintas, S. Das, A. McAuley, and W. Chen, "Marconinet supporting streaming media over localized wireless multicast," in *International Workshop of Mobile E-Commerce*, (Atlanta, Georgia), Sept. 2002.

[43] H. Schulzrinne and W. Jiang, "Quality of service - applications," in *NSF ITR Quality of Service Workshop*, (Annapolis, Maryland), Mar. 2002.

[44] H. Schulzrinne, "Interdomain and end-to-end QoS issues," in *NSF ITR Quality of Service Workshop*, (Annapolis, Maryland), Mar. 2002.

[45] L. Amini and H. Schulzrinne, "Observations from router-level Internet traces," in *DIMACS Workshop on Internet and WWW Measurement, Mapping and Modeling*, (Piscataway, New Jersey), Feb. 2002.

[46] K. Koguchi, W. Jiang, and H. Schulzrinne, "QoS measurement of VoIP end-points," in *IEICE Group meeting on Network Systems*, (Matsuyama, Japan), Dec. 2002.

[47] W. Zhao and H. Schulzrinne, "ARMS - automated replication for meshed servers," in *3rd NMADS (New York Metra Area Distributed Systems) Day*, (New York, NY), Apr. 2001.

[48] E. Hahne, P. Pan, and H. Schulzrinne, "Scalable resource reservation for Internet QoS," in *DIMACS Workshop on QoS*, (Rutgers University), Feb. 2001.

[49] W. Jiang, J. Lennox, H. Schulzrinne, and K. Singh, "Towards junking the PBX: deploying IP telephony," in *Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV)*, (Port Jefferson, New York), June 2001.

[50] K. Singh, G. Nair, and H. Schulzrinne, "Centralized conferencing using SIP," in *Internet Telephony Workshop*, (New York), Apr. 2001.

[51] X. Wu and H. Schulzrinne, "Where should services reside in Internet telephony systems?," in *IP Telecom Services Workshop*, (Atlanta, Georgia), pp. 35–40, Sept. 2000.

[52] K. Singh and H. Schulzrinne, "Unified messaging using SIP and RTSP," in *IP Telecom Services Workshop*, (Atlanta, Georgia), pp. 31–37, Sept. 2000.

[53] D. Sisalem and H. Schulzrinne, "The direct adjustment algorithm: A TCP-Friendly adaptation scheme," in *Quality of Future Internet Services*, (Berlin, Germany), Sept. 2000.

[54] X. Wang and H. Schulzrinne, "Performance study of congestion price based adaptive service," in *Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV)*, (Chapel Hill, North Carolina), pp. 1–10, June 2000.

[55] W. Jiang and H. Schulzrinne, "Modeling of packet loss and delay and their effect on real-time multimedia service quality," in *Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV)*, June 2000.

[56] H. Schulzrinne, "Internet telephony: A second chance," in *IP-Telephony Workshop (IPtel)*, (Berlin, Germany), Apr. 2000.

[57] K. Singh and H. Schulzrinne, "Interworking between SIP/SDP and H.323," in *IP-Telephony Workshop (IPtel)*, (Berlin, Germany), Apr. 2000.

[58] T. Eyers and H. Schulzrinne, "Predicting Internet telephony call setup delay," in *IP-Telephony Workshop (IPtel)*, (Berlin, Germany), Apr. 2000.

[59] J. Lennox and H. Schulzrinne, "The call processing language: User control of internet telephony services," in *Lucent Technologies XML Day*, (Murray Hill, NJ), Feb. 2000.

[60] H. Schulzrinne, "Feature interaction in Internet telephony," in *Feature Interaction in Telecommunication Networks IV*, (Montreal, Canada), p. 371, June 1997.

[61] H. Schulzrinne, "Scaling issues for the integrated services Internet," in *DIMACS: Workshop Architecture and Algorithmic Aspects of Communication Networks*, (New Brunswick, New Jersey), Jan. 1997.

[62] H. Schulzrinne and D. Sisalem, "Interaction of ATM and IP congestion control," in *Workshop on Integration of IP and ATM*, (St. Louis, Missouri), Nov. 1996.

[63] H. Schulzrinne, "Issues for session invitation protocols," in *Internet Engineering Task Force (IETF) Meeting*, (Montreal, California), June 1996.

[64] H. Schulzrinne, "Internet telephony – towards the integrated services Internet," in *IEEE Workshop on Internet Telephony*, (Utrecht, The Netherlands), Feb. 1996.

[65] H. Schulzrinne, J. Brassil, and A. K. Choudhury, "Internet access to IEEE journals: The september trial," in *Documents in Public Networks — Applications and Experiences (Dokumente in öffentlichen Netzen – Anwendungen und Erfahrungen)*, (Darmstadt, Germany), Nov. 1995.

[66] H. Schulzrinne, "Whither WWW — status, problems, directions," in *WWW für kommerzielle Anwender und kommerzielle Informationsanbieter im Internet (Supercomputer Tutorial)*, (Mannheim, Germany), June 1995.

[67] I. Busse, B. Deffner, and H. Schulzrinne, "Dynamic QoS control of multimedia applications based on RTP," in *1st International Workshop on High Speed Networks and Open Distributed Platforms*, (St. Petersburg, Russia), June 1995.

[68] H. Schulzrinne, "ATM: dangerous at any speed?," in *IEEE Gigabit Networking Workshop*, (Boston, Massachusetts), Apr. 1995.

[69] H. Schulzrinne, "QOS for real-time services: playout delay and application control," in *46th RACE Concertation Meeting (RCM)*, (Brussels, Belgium), Mar. 1995.

[70] H. Schulzrinne, "Quality of service in integrated networks." TUBKOM Seminar Series, Feb. 1995.

[71] L. Kleinrock, J. P. Sterbenz, N. F. Maxemchuk, S. S. Lam, P. Steenkiste, and H. Schulzrinne, "The national exchange for networked information systems: A white paper," in *Gigabit Networking Workshop*, (Toronto, Ontario), June 1994.

[72] H. Schulzrinne, "RTP: the real-time transport protocol," in *MCNC 2nd Packet Video Workshop*, Vol. 2, (Research Triangle Park, North Carolina), Dec. 1992.

[73] J. F. Kurose, D. F. Towsley, and H. Schulzrinne, "Scheduling policies for supporting real-time traffic in wide-area computer networks," in *Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV)*, (Berkeley, California), Nov. 1990. TR-90-062.

INTERNET RFCS AND DRAFTS

Note: Date shown is that of latest revision, not first version.

[1] S. Baset, H. Schulzrinne, and E. Shim, "A protocol for implementing various DHT algorithms," Internet Draft draft-baset-sipping-p2pcommon, Internet Engineering Task Force, Oct. 2006. Work in progress.

[2] G. Camarillo, H. Schulzrinne, and E. Burger, "The source and sink attributes for the session description protocol," Internet Draft draft-camarillo-mmusic-source-sink-01, Internet Engineering Task Force, Aug. 2003. Work in progress.

[3] A. Forte, S. Shin, and H. Schulzrinne, "Passive duplicate address detection for the dynamic host configuration protocol for IPv4 (DHCPv4)," Internet Draft draft-forte-dhc-passive-dad-01, Internet Engineering Task Force, Mar. 2006. Work in progress.

[4] X. Fu and M. et. al., "Mobility issues in next steps in signaling (NSIS)," Internet Draft draft-fu-nsis-mobility-01.txt,, Internet Engineering Task Force, Oct. 2003. Work in progress.

[5] H. Schulzrinne, S. Petrack, and T. Taylor, "Definition of events for Channel-Oriented telephony signalling," Internet Draft draft-ietf-avt-rfc2833biscas, IETF, Jan. 2007. Work in progress.

[6] H. Schulzrinne, S. Petrack, and T. Taylor, "Definition of events for modem, FAX, and text telephony signals," Internet Draft draft-ietf-avt-rfc2833bisdata, IETF, Feb. 2005. Work in progress.

[7] H. Schulzrinne and R. Marshall, "Requirements for emergency context resolution with internet technologies," Internet Draft draft-ietf-ecrit-requirements-12, Internet Engineering Task Force, Aug. 2006. Work in progress.

[8] H. Schulzrinne, "A uniform resource name (URN) for services," Internet Draft draft-ietf-ecrit-service-urn, Internet Engineering Task Force, Aug. 2006. Work in progress.

[9] T. Taylor, H. Tschofenig, H. Schulzrinne, and M. Shanmugam, "Security threats and requirements for emergency call marking and mapping," Internet Draft draft-ietf-ecrit-security-threats-03, Internet Engineering Task Force, July 2006. Work in progress.

[10] H. Schulzrinne, J. Polk, and H. Tschofenig, "A dynamic host configuration protocol (DHCP) based Location-to-Service translation protocol (LoST) discovery procedure," Internet Draft draft-ietf-ietf-ecrit-dhc-lost-discovery, Internet Engineering Task Force, Mar. 2007. Work in progress.

[11] H. Tschofenig and H. Schulzrinne, "GEOPRIV layer 7 location configuration protocol; problem statement and requirements," Internet Draft draft-ietf-geopriv-l7-lcp-ps, Internet Engineering Task Force, Jan. 2007. Work in progress.

[12] H. Schulzrinne and H. Tschofening, "Location types registry," Internet Draft draft-ietf-geopriv-location-types-registry-05, Internet Engineering Task Force, Mar. 2006. Work in progress.

[13] H. Schulzrinne, H. Tschofenig, J. Morris, J. Cuellar, and J. Polk, "Policy rules for disclosure and modification of geographic information," Internet Draft draft-ietf-geopriv-policy-07, Internet Engineering Task Force, Oct. 2005. Work in progress.

[14] H. Schulzrinne, "Real time streaming protocol (RTSP)," Internet Draft draft-ietf-mmusic-rfc2326bis-05.txt,.ps,, Internet Engineering Task Force, Oct. 2003. Work in progress.

[15] H. Schulzrinne and R. Hancock, "GIMPS: general internet messaging protocol for signaling," Internet Draft draft-ietf-nsis-ntlp-11, Internet Engineering Task Force, Aug. 2006. Work in progress.

[16] H. Schulzrinne, "is-composing indication for instant messaging using the session initiation protocol (SIP)," Internet Draft draft-ietf-simple-iscomposing, Internet Engineering Task Force, Mar. 2004. Work in progress.

[17] J. Rosenberg, "Guidelines for authors of extensions to the session initiation protocol (SIP)," Internet Draft draft-ietf-sip-guidelines-07, Internet Engineering Task Force, Oct. 2003. Work in progress.

[18] H. Schulzrinne, "Emergency services URI for the session initiation protocol," Internet Draft draft-ietf-sipping-sos-00, Internet Engineering Task Force, Feb. 2004. Work in progress.

[19] J. Rosenberg, H. Schulzrinne, and B. Suter, "Wide area network service location," internet draft, Internet Engineering Task Force, Dec. 1997. Work in progress.

[20] J. Lee and H. Schulzrinne, "SIP URI service discovery using DNS-SD," Internet Draft draft-lee-sip-dns-sd-uri, Internet Engineering Task Force, Feb. 2007. Work in progress.

[21] J. Lennox, H. Schulzrinne, J. Nieh, and R. Baratto, "Protocols for application and desktop sharing," Internet Draft draft-lennox-avt-app-sharing, IETF, Dec. 2004. Work in progress.

[22] S. Narayanan, H. Schulzrinne, and A. Kundaje, "A diameter accounting application for the session initiation protocol," internet draft, Internet Engineering Task Force, Aug. 2002. Work in progress.

[23] P. Pan and H. Schulzrinne, "An evaluation on RSVP transport mechanism," internet draft, Internet Engineering Task Force, Mar. 2003. Work in progress.

[24] P. Pan, E. Hahne, and H. Schulzrinne, "BGRP: a framework for scalable resource reservation," internet draft, Internet Engineering Task Force, Jan. 2000. Work in progress.

[25] J. Rosenberg, J. Weinberger, and H. Schulzrinne, "NAT friendly SIP," internet draft, Internet Engineering Task Force, July 2001. Work in progress.

[26] J. Rosenberg, D. Drew, and H. Schulzrinne, "Getting SIP through firewalls and NATs," internet draft, Internet Engineering Task Force, Feb. 2000. Work in progress.

[27] H. Schulzrinne *et al.*, "RADIUS accounting for SIP servers," internet draft, Internet Engineering Task Force, Feb. 2002. Work in progress.

[28] H. Schulzrinne, "Synchronizing Location-to-Service translation (LoST) servers," Internet Draft draft-schulzrinne-ecrit-lost-sync, Internet Engineering Task Force, Nov. 2006. Work in progress.

[29] H. Schulzrinne, "A location reference event package for the session initiation protocol (SIP)," Internet Draft draft-schulzrinne-geopriv-locationref, Internet Engineering Task Force, Oct. 2006. Work in progress.

[30] H. Schulzrinne, "RELO: retrieving end system location information," Internet Draft draft-schulzrinne-geopriv-relo, Internet Engineering Task Force, Mar. 2007. Work in progress.

[31] H. Schulzrinne, "Composing presence information," Internet Draft draft-schulzrinne-simple-composition-00, Internet Engineering Task Force, July 2005. Work in progress.

[32] H. Schulzrinne, J. Lennox, J. Nieh, and R. Baratto, "Sharing and remote access to applications," Internet Draft draft-schulzrinne-mmusic-sharing, IETF, Sept. 2004. Work in progress.

[33] H. Schulzrinne, "Requirements for session initiation protocol (SIP)-based emergency calls," internet draft, Internet Engineering Task Force, Feb. 2003. Work in progress.

[34] H. Schulzrinne and B. Rosen, "Emergency services for internet telephony systems," Internet Draft draft-schulzrinne-sipping-emergency-arch-00, Internet Engineering Task Force, Feb. 2004. Work in progress.

[35] R. Shacham, H. Schulzrinne, S. Thakolsri, and W. Kellerer, "Session initiation protocol (SIP) session mobility," Internet Draft draft-shacham-sipping-session-mobility, IETF, Feb. 2005. Work in progress.

[36] C. Shen, H. Schulzrinne, S.-H. Lee, and J. Bang, "Internet routing dynamics and NSIS related considerations," internet draft, IETF, Oct. 2004. Work in progress.

[37] C. Shen, H. Schulzrinne, S.-H. Lee, and J. Bang, "NSIS operation over IP tunnels," Internet Draft draft-shen-nsis-tunnel-02, Internet Engineering Task Force, Mar. 2006. Work in progress.

[38] V. Singh, H. Schulzrinne, and H. Tschofenig, "Dynamic feature extensions to the presence information data format location object (PIDF-LO)," Internet Draft draft-singh-geopriv-pidf-lo-dynamic, Internet Engineering Task Force, Feb. 2007. Work in progress.

[39] K. Singh and H. Schulzrinne, "Data format and interface to an external peer-to-peer network for SIP location service," Internet Draft draft-singh-p2p-sip, Internet Engineering Task Force, Dec. 2006. Work in progress.

[40] V. Singh, H. Schulzrinne, and P. Boni, "Vehicle info event package," Internet Draft draft-singh-simple-vehicle-info, Internet Engineering Task Force, Mar. 2007. Work in progress.

[41] K. Singh and H. Schulzrinne, "Interworking between SIP/SDP and H.323," internet draft, Internet Engineering Task Force, May 2000. Work in progress.

[42] H. Tschofenig, D. Wing, H. Schulzrinne, T. Froment, and G. Dawirs, "Anti-SPIT : A document format for expressing Anti-SPIT authorization policies," Internet Draft draft-tschofenig-sipping-spit-policy, Internet Engineering Task Force, Feb. 2007. Work in progress.

[43] H. Tschofenig, H. Schulzrinne, D. Wing, J. Rosenberg, and D. Schwartz, "A framework to tackle spam and unwanted communication for internet telephony," Internet Draft draft-tschofenig-sipping-framework-spit-reduction, Internet Engineering Task Force, Jan. 1993.

[44] H. Tschofenig, G. Dawirs, T. Froment, D. Wing, D. Wing, and H. Schulzrinne, "Requirements for authorization policies to tackle spam and unwanted communication for internet telephony," Internet Draft draft-froment-sipping-spit-requirements, Internet Engineering Task Force, Feb. 2008.

[45] D. Trossen and H. Schulzrinne, "On-Demand access authorization for SIP event=20 subscriptions," Internet Draft draft-trossen-sipping-ondemand-00, Internet Engineering Task Force, Oct. 2003. Work in progress.

[46] S. Tsang, "Requirements for networked appliances: Wide-Area access, control, and interworking," internet draft, Internet Engineering Task Force, Sept. 2000. Work in progress.

[47] S. Tsang, "SIP extensions for communicating with networked appliances," internet draft, Internet Engineering Task Force, Nov. 2000. Work in progress.

[48] H. Tschofenig and H. Schulzrinne, "RSVP domain of interpretation for ISAKMP," Internet Draft draft-tschofenig-rsvp-doi-01, Internet Engineering Task Force, Oct. 2003. Work in progress.

[49] X. Wu and H. Schulzrinne, "Location-switch for call processing language (CPL)," internet draft, Internet Engineering Task Force, Feb. 2004. Work in progress.

[50] X. Wu, H. Schulzrinne, J. Lennox, and J. Rosenberg, "CPL extensions for presence," internet draft, Internet Engineering Task Force, June 2001. Work in progress.

[51] W. Zhao and H. Schulzrinne, "Locating IP-to-Public switched telephone network (PSTN) telephony gateways via SLP," internet draft, Internet Engineering Task Force, Feb. 2004. Work in progress.

[52] W. Zhao and H. Schulzrinne, "Enabling global service attributes in the service location protocol," internet draft, Internet Engineering Task Force, Oct. 2005. Work in progress.

[53] H. Schulzrinne, L. Liess, H. Tschofenig, B. Stark, and A. KÃ¼tt, "Location hiding: Problem statement and requirements," Internet Draft draft-schulzrinne-ecrit-location-hiding-req, Internet Engineering Task Force, Mar. 2008.

[54] H. Schulzrinne, S. McCann, G. Bajko, and H. Tschofenig, "Extensions to the emergency services architecture for dealing with unauthenticated and unauthorized devices," Internet Draft draft-schulzrinne-ecrit-unauthenticated-access-02, Internet Engineering Task Force, Feb. 2008.

[55] H. Schulzrinne, "Applications and media information (AMI) extension to the presence information data format," Internet Draft draft-schulzrinne-simple-ami-00, Internet Engineering Task Force, Nov. 2007.

[56] R. Barnes, M. Lepinski, H. Tschofenig, and H. Schulzrinne, "Security requirements for the geopriv location system," Internet Draft draft-barnes-geopriv-lo-sec-02, Internet Engineering Task Force, Feb. 2008.

[57] M. Barnes, C. Boulton, and H. Schulzrinne, "Centralized conferencing manipulation protocol," Internet Draft draft-barnes-xcon-ccmp-04, Internet Engineering Task Force, Feb. 2008.

[58] S. Baset, H. Schulzrinne, and M. Matuszewski, "Peer-to-Peer protocol (P2PP)," Internet Draft draft-baset-p2psip-p2pp, Internet Engineering Task Force, Nov. 2007.

[59] C. Jennings, B. Lowekamp, E. Rescorla, J. Rosenberg, S. Baset, and H. Schulzrinne, "REsource LOcation and discovery (RELOAD)," Internet Draft draft-bryan-p2psip-reload, Internet Engineering Task Force, Feb. 2008.

[60] A. Dutta, H. Yokota, T. Chiba, and H. Schulzrinne, "ProxyMIP extension for Inter-MAG route optimization," Internet Draft draft-dutta-netlmm-pmipro-00, Internet Engineering Task Force, Feb. 2008.

[61] A. Forte and H. Schulzrinne, "Location-to-Service translation protocol (LoST) extensions," Internet Draft draft-forte-ecrit-lost-extensions, Internet Engineering Task Force, Mar. 2008.

[62] M. GarcÃa-MartÃn, H. Tschofenig, and H. Schulzrinne, "Indirect presence publication with the session initiation protocol (SIP)," Internet Draft draft-garcia-simple-indirect-presence-publish, Internet Engineering Task Force, Feb. 2008.

[63] V. Hilt, I. Widjaja, and D. Malas, "Session initiation protocol (SIP) overload control," Internet Draft draft-hilt-sipping-overload, Internet Engineering Task Force, Feb. 2008.

[64] A. Houri, S. Parameswar, E. Aoki, V. Singh, and H. Schulzrinne, "Scaling requirements for presence in SIP/SIMPLE," Internet Draft draft-houri-sipping-presence-scaling-requirements, Internet Engineering Task Force, Nov. 2007.

[65] B. Rosen, H. Schulzrinne, B. Rosen, and A. Newton, "Framework for emergency calling using internet multimedia," Internet Draft draft-ietf-ecrit-framework, Internet Engineering Task Force, Feb. 2008.

[66] A. Houri, E. Aoki, S. Parameswar, T. Rang, V. Singh, and H. Schulzrinne, "Presence interdomain scaling analysis for SIP/SIMPLE," Internet Draft draft-ietf-simple-interdomain-scaling-analysis, Internet Engineering Task Force, Feb. 2008.

[67] A. Houri, S. Parameswar, E. Aoki, V. Singh, and H. Schulzrinne, "Scaling requirements for presence in SIP/SIMPLE," Internet Draft draft-ietf-sipping-presence-scaling-requirements, Internet Engineering Task Force, Feb. 2008.

[68] A. Dutta, V. Fajardo, Y. Ohba, K. Taniuchi, and H. Schulzrinne, "A framework of Media-Independent Pre-Authentication (MPA) for inter-domain handover optimization," Internet Draft draft-irtf-mobopts-mpa-framework, Internet Engineering Task Force, Feb. 2008.

[69] A. Melnikov, H. Schulzrinne, and Q. Sun, "Sieve notification mechanism: SIP MESSAGE," Internet Draft draft-melnikov-sieve-notify-sip-message, Internet Engineering Task Force, Feb. 2008.

[70] J. Seedorf, S. Niccolini, and H. Schulzrinne, "Spam score for SIP: a proposal for semantics," Internet Draft draft-seedorf-sipping-spam-score-semantics, Internet Engineering Task Force, Feb. 2008.

[71] H. Tschofenig, J. Ott, H. Schulzrinne, T. Henderson, and G. Camarillo, "Interaction between SIP and HIP," Internet Draft draft-tschofenig-hiprg-host-identities, Internet Engineering Task Force, Feb. 2008.

[72] B. Rosen, H. Schulzrinne, and H. Tschofenig, "Session initiation protocol (SIP) event package for the common alerting protocol (CAP)," Internet Draft draft-rosen-sipping-cap, Internet Engineering Task Force, May 2008.

[73] J. Winterbottom, H. Tschofenig, H. Schulzrinne, M. Thomson, and M. Dawson, "An HTTPS location dereferencing protocol using HELD," Internet Draft draft-winterbottom-geopriv-deref-protocol, Internet Engineering Task Force, Nov. 2007.

[74] D. Wong, A. Dutta, and H. Schulzrinne, "Simultaneous mobility problem statement," Internet Draft draft-wong-mext-simultaneous-ps, Internet Engineering Task Force, Feb. 2008.

[75] M. GarcÃa-MartÃn and H. Schulzrinne, "Notification of general events using the session initiation protocol (SIP) event notification framework," Internet Draft draft-garcia-sipping-general-events, Internet Engineering Task Force, May 2007.

[76] S. Greco Polito and H. Schulzrinne, "Authentication, authorization, accounting and billing of roaming users using SAML," Internet Draft draft-greco-sipping-roaming, Internet Engineering Task Force, July 2007.

[77] R. Shacham and H. Schulzrinne, "HTTP header for future correspondence addresses," Internet Draft draft-shacham-http-corr-uris, Internet Engineering Task Force, May 2007.

[78] H. Tschofenig and H. Schulzrinne, "Emergency services architecture overview: Sharing responsibilities," Internet Draft draft-tschofenig-ecrit-architecture-overview, Internet Engineering Task Force, July 2007.

[79] H. Tschofenig and H. Schulzrinne, "A GEOPRIV HTTPS using protocol," Internet Draft draft-tschofenig-geopriv-http-using-protocol, Internet Engineering Task Force, July 2007.

[80] A. Forte and H. Schulzrinne, "Classification of location-based services," Internet Draft draft-forte-ecrit-service-classification, Internet Engineering Task Force, May 2008.

[81] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, "RTP: a transport protocol for Real-Time applications," RFC 1889, Internet Engineering Task Force, Jan. 1996.

[82] H. Schulzrinne, "RTP profile for audio and video conferences with minimal control," RFC 1890, Internet Engineering Task Force, Jan. 1996.

[83] H. Schulzrinne, A. Rao, and R. Lanphier, "Real time streaming protocol (RTSP)," RFC 2326, Internet Engineering Task Force, Apr. 1998.

[84] H. Lu, M. Krishnaswamy, L. Conroy, S. M. Bellovin, F. Burg, A. DeSimone, K. Tewani, and P. J. Davidson, "Toward the PSTN/Internet Inter-Networking–Pre-PINT implementations," RFC 2458, Internet Engineering Task Force, Nov. 1998.

[85] M. Handley, H. Schulzrinne, E. M. Schooler, and J. Rosenberg, "SIP: session initiation protocol," RFC 2543, Internet Engineering Task Force, Mar. 1999.

[86] J. Rosenberg and H. Schulzrinne, "An RTP payload format for generic forward error correction," RFC 2733, Internet Engineering Task Force, Dec. 1999.

[87] J. Rosenberg and H. Schulzrinne, "Sampling of the group membership in RTP," RFC 2762, Internet Engineering Task Force, Feb. 2000.

[88] J. Lennox and H. Schulzrinne, "Call processing language framework and requirements," RFC 2824, Internet Engineering Task Force, May 2000.

[89] H. Schulzrinne and S. Petrack, "RTP payload for DTMF digits, telephony tones and telephony signals," RFC 2833, Internet Engineering Task Force, May 2000.

[90] J. Rosenberg and H. Schulzrinne, "A framework for telephony routing over IP," RFC 2871, Internet Engineering Task Force, June 2000.

[91] J. Rosenberg and H. Schulzrinne, "Registration of parityfec MIME types," RFC 3009, Internet Engineering Task Force, Nov. 2000.

[92] J. Lennox, H. Schulzrinne, and J. Rosenberg, "Common gateway interface for SIP," RFC 3050, Internet Engineering Task Force, Jan. 2001.

[93] C. E. Perkins, J. Rosenberg, and H. Schulzrinne, "RTP testing strategies," RFC 3158, Internet Engineering Task Force, Aug. 2001.

[94] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. R. Johnston, J. Peterson, R. Sparks, M. Handley, and E. M. Schooler, "SIP: session initiation protocol," RFC 3261, Internet Engineering Task Force, June 2002.

[95] J. Rosenberg and H. Schulzrinne, "Reliability of provisional responses in session initiation protocol (SIP)," RFC 3262, Internet Engineering Task Force, June 2002.

[96] J. Rosenberg and H. Schulzrinne, "Session initiation protocol (SIP): locating SIP servers," RFC 3263, Internet Engineering Task Force, June 2002.

[97] J. Rosenberg and H. Schulzrinne, "An Offer/Answer model with session description protocol (SDP)," RFC 3264, Internet Engineering Task Force, June 2002.

[98] H. Schulzrinne and B. Volz, "Dynamic host configuration protocol (DHCPv6) options for session initiation protocol (SIP) servers," RFC 3319, Internet Engineering Task Force, July 2003.

[99] H. Schulzrinne, D. Oran, and G. Camarillo, "The reason header field for the session initiation protocol (SIP)," RFC 3326, Internet Engineering Task Force, Dec. 2002.

[100] H. Schulzrinne, "Dynamic host configuration protocol (DHCP-for-IPv4) option for session initiation protocol (SIP) servers," RFC 3361, Internet Engineering Task Force, Aug. 2002.

[101] G. Camarillo, G. Eriksson, J. Holler, and H. Schulzrinne, "Grouping of media lines in the session description protocol (SDP)," RFC 3388, Internet Engineering Task Force, Dec. 2002.

[102] W. Zhao, H. Schulzrinne, E. Guttman, C. Bisdikian, and W. Jerome, "Select and sort extensions for the service location protocol (SLP)," RFC 3421, Internet Engineering Task Force, Nov. 2002.

[103] B. Campbell, J. Rosenberg, and Y. E. E. Liu, eds., "Session initiation protocol (SIP) extension for instant messaging," RFC 3428, Internet Engineering Task Force, Dec. 2002.

[104] H. Schulzrinne, "Requirements for resource priority mechanisms for the session initiation protocol (SIP)," RFC 3487, Internet Engineering Task Force, Feb. 2003.

[105] W. Zhao, H. Schulzrinne, and E. Guttman, "Mesh-enhanced service location protocol (mSLP)," RFC 3528, Internet Engineering Task Force, Apr. 2003.

[106] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, "RTP: a transport protocol for Real-Time applications," RFC 3550, Internet Engineering Task Force, July 2003.

[107] H. Schulzrinne and S. Casner, "RTP profile for audio and video conferences with minimal control," RFC 3551, Internet Engineering Task Force, July 2003.

[108] J. Rosenberg and H. Schulzrinne, "An extension to the session initiation protocol (SIP) for symmetric response routing," RFC 3581, Internet Engineering Task Force, Aug. 2003.

[109] J. Rosenberg, J. Peterson, H. Schulzrinne, and G. Camarillo, "Best current practices for third party call control (3pcc) in the session initiation protocol (SIP)," RFC 3725, Internet Engineering Task Force, Apr. 2004.

[110] W. Zhao, H. Schulzrinne, E. Guttman, C. Bisdikian, and W. Jerome, "Remote service discovery in the service location protocol (SLP) via DNS SRV," RFC 3832, Internet Engineering Task Force, July 2004.

[111] J. Rosenberg, P. Kyzivat, and H. Schulzrinne, "Indicating user agent capabilities in the session initiation protocol (SIP)," RFC 3840, Internet Engineering Task Force, Aug. 2004.

[112] J. Rosenberg, H. Schulzrinne, and P. Kyzivat, "Caller preferences for the session initiation protocol (SIP)," RFC 3841, Internet Engineering Task Force, Aug. 2004.

[113] J. Lennox, X. Wu, and H. Schulzrinne, "Call processing language (CPL): a language for user control of internet telephony services," RFC 3880, Internet Engineering Task Force, Oct. 2004.

[114] G. Camarillo and H. Schulzrinne, "Early media and ringing tone generation in the session initiation protocol (SIP)," RFC 3960, Internet Engineering Task Force, Dec. 2004.

[115] H. Schulzrinne, "The tel URI for telephone numbers," RFC 3966, Internet Engineering Task Force, Dec. 2004.

[116] H. Schulzrinne, "Indication of message composition for instant messaging," RFC 3994, Internet Engineering Task Force, Jan. 2005.

[117] G. Camarillo, E. W. Burger, H. Schulzrinne, and A. van Wijk, "Transcoding services invocation in the session initiation protocol (SIP) using third party call control (3pcc)," RFC 4117, Internet Engineering Task Force, June 2005.

[118] H. Schulzrinne and C. Agboh, "Session initiation protocol (SIP)-H.323 interworking requirements," RFC 4123, Internet Engineering Task Force, July 2005.

[119] J. Rosenberg, H. Schulzrinne, and G. Camarillo, "The stream control transmission protocol (SCTP) as a transport for the session initiation protocol (SIP)," RFC 4168, Internet Engineering Task Force, Oct. 2005.

[120] J. Rosenberg, H. Schulzrinne, and R. Mahy, "An INVITE-Initiated dialog event package for the session initiation protocol (SIP)," RFC 4235, Internet Engineering Task Force, Nov. 2005.

[121] P. Koskelainen, J. Ott, H. Schulzrinne, and X. Wu, "Requirements for floor control protocols," RFC 4376, Internet Engineering Task Force, Feb. 2006.

[122] H. Schulzrinne and J. Polk, "Communications resource priority for the session initiation protocol (SIP)," RFC 4412, Internet Engineering Task Force, Feb. 2006.

[123] Y. Nomura, R. Walsh, J.-P. Luoma, H. Asaeda, and H. Schulzrinne, "A framework for the usage of internet media guides (IMGs)," RFC 4435, Internet Engineering Task Force, Apr. 2006.

[124] Y. Nomura, R. Walsh, J.-P. Luoma, J. Ott, and H. Schulzrinne, "Requirements for internet media guides (IMGs)," RFC 4473, Internet Engineering Task Force, May 2006.

[125] R. J. Sparks, A. Hawrylyshen, A. Johnston, J. Rosenberg, and H. Schulzrinne, "Session initiation protocol (SIP) torture test messages," RFC 4475, Internet Engineering Task Force, May 2006.

[126] H. Schulzrinne, V. Gurbani, P. Kyzivat, and J. Rosenberg, "RPID: rich presence extensions to the presence information data format (PIDF)," RFC 4480, Internet Engineering Task Force, July 2006.

[127] H. Schulzrinne, "Timed presence extensions to the presence information data format (PIDF) to indicate status information for past and future time intervals," RFC 4481, Internet Engineering Task Force, July 2006.

[128] H. Schulzrinne, "CIPID: contact information for the presence information data format," RFC 4482, Internet Engineering Task Force, July 2006.

[129] J. Rosenberg and H. Schulzrinne, "Guidelines for authors of extensions to the session initiation protocol (SIP)," RFC 4485, Internet Engineering Task Force, May 2006.

[130] H. Schulzrinne and H. Tschofenig, "Location types registry," RFC 4589, Internet Engineering Task Force, July 2006.

[131] H. Schulzrinne, "Dynamic host configuration protocol (DHCPv4 and DHCPv6) option for civic addresses configuration information," rfc, Internet Engineering Task Force, Oct. 2006.

[132] H. Schulzrinne and T. Taylor, "RTP payload for DTMF digits, telephony tones, and telephony signals," RFC 4733, Internet Engineering Task Force, Dec. 2006.

[133] H. Schulzrinne and T. Taylor, "Definition of events for modem, fax, and text telephony signals," RFC 4734, Internet Engineering Task Force, Dec. 2006.

[134] H. Schulzrinne, H. Tschofenig, J. Morris, J. R. Cuellar, J. Polk, and J. Rosenberg, "Common policy: A document format for expressing privacy preferences," RFC 4745, Internet Engineering Task Force, Feb. 2007.

[135] H. Schulzrinne, "Dynamic host configuration protocol (DHCPv4 and DHCPv6) option for civic addresses configuration information," RFC 4776, Internet Engineering Task Force, Nov. 2006.

[136] H. Schulzrinne and R. S. Marshall, "Requirements for emergency context resolution with internet technologies," RFC 5012, Internet Engineering Task Force, Jan. 2008.

[137] H. Schulzrinne, "A uniform resource name (URN) for emergency and other Well-Known services," RFC 5031, Internet Engineering Task Force, Jan. 2008.

[138] T. Taylor, H. Tschofenig, H. Schulzrinne, and M. Shanmugam, "Security threats and requirements for emergency call marking and mapping," RFC 5069, Internet Engineering Task Force, Jan. 2008.

[139] T. Hardie, A. L. Newton, H. Schulzrinne, and H. Tschofenig, "LoST: a Location-to-Service translation protocol," RFC 5222, Internet Engineering Task Force, Aug. 2008.

[140] H. Schulzrinne, J. Polk, and H. Tschofenig, "Discovering Location-to-Service translation (LoST) servers using the dynamic host configuration protocol (DHCP)," RFC 5223, Internet Engineering Task Force, Aug. 2008.

[141] H. Schulzrinne and T. Taylor, "Definition of events for Channel-Oriented telephony signalling," RFC 5244, Internet Engineering Task Force, June 2008.

[142] H. Schulzrinne, "Location-to-URL mapping architecture and framework," RFC 5582, Internet Engineering Task Force, Sept. 2009.

[143] R. Shacham, H. Schulzrinne, S. Thakolsri, and W. Kellerer, "Session initiation protocol (SIP) session mobility," RFC 5631, Internet Engineering Task Force, Oct. 2009.

[144] H. Tschofenig and H. Schulzrinne, "GEOPRIV layer 7 location configuration protocol: Problem statement and requirements," RFC 5687, Internet Engineering Task Force, Mar. 2010.

[145] H. Schulzrinne, E. Marocco, and E. Ivov, "Security issues and solutions in Peer-to-Peer systems for realtime communications," RFC 5765, Internet Engineering Task Force, Feb. 2010.

[146] G. Camarillo and H. Schulzrinne, "The session description protocol (SDP) grouping framework," RFC 5888, Internet Engineering Task Force, June 2010.

[147] H. Schulzrinne, V. K. Singh, H. Tschofenig, and M. Thomson, "Dynamic extensions to the presence information data format location object (PIDF-LO)," RFC 5962, Internet Engineering Task Force, Sept. 2010.

[148] H. Schulzrinne and R. E. Hancock, "GIST: general internet signalling transport," RFC 5971, Internet Engineering Task Force, Oct. 2010.

[149] C. Shen, H. Schulzrinne, S.-H. Lee, and J. H. Bang, "NSIS operation over IP tunnels," RFC 5979, Internet Engineering Task Force, Mar. 2011.

[150] A. Dutta, V. Fajardo, Y. Ohba, K. Taniuchi, and H. Schulzrinne, "A framework of media-independent pre-authentication (mpa) for inter-domain handover optimization," Request for Comments 6252, Internet Engineering Task Force, June 2011.

[151] R. Barnes, M. Lepinski, A. Cooper, J. Morris, H. Tschofenig, and H. Schulzrinne, "An architecture for location and location privacy in internet applications," Request for Comments 6280, Internet Engineering Task Force, July 2011.

[152] B. Rosen, H. Schulzrinne, J. Polk, and A. Newton, "Framework for emergency calling using Internet multimedia," Request for Comments 6443, Internet Engineering Task Force, Dec. 2011.

[153] A. Forte and H. Schulzrinne, "Location-to-service translation (LoST) protocol extensions," Request for Comments 6451, Internet Engineering Task Force, Dec. 2011.

[154] M. Barnes, C. Boulton, S. P. Romano, and H. Schulzrinne, "Centralized conferencing manipulation protocol," Request for Comments 6503, Internet Engineering Task Force, Mar. 2012.

[155] H. Schulzrinne and H. Tschofenig, "Synchronizing service boundaries and <mapping> elements based on the location-to-service translation (LoST) protocol," Request for Comments 6739, Internet Engineering Task Force, Oct. 2012.

[156] J. Winterbottom, H. Tschofenig, H. Schulzrinne, and M. Thomson, "A location dereference protocol using HTTP-enabled location delivery (HELD)," Request for Comments 6753, Internet Engineering Task Force, Oct. 2012.

[157] H. Schulzrinne, H. Tschofenig, J. R. Cuellar, J. Polk, J. B. Morris, and M. Thomason, "Geolocation policy: A document format for expressing privacy preferences for location information," Request for Comments 6772, Internet Engineering Task Force, Jan. 2013.

[158] C. Jennings, B. Lowekamp, E. Rescorla, S. Baset, and H. Schulzrinne, "Resource location and discovery (RELOAD) base protocol," Request for Comments 6940, Internet Engineering Task Force, Jan. 2014.

[159] H. Schulzrinne, H. Tschofenig, C. Holmberg, and M. Patel, "Public safety answering point (PSAP) callback," Request for Comments 7090, Internet Engineering Task Force, Apr. 2014.

[160] C. Shen, H. Schulzrinne, and A. Koike, "A session initiation protocol (SIP) load-control event package," Request for Comments 7200, Internet Engineering Task Force, Apr. 2014.

[161] V. Gurbani, V. Hilt, and H. Schulzrinne, "Session Initiation Protocol (SIP) overload control," Request for Comments 7339, Internet Engineering Task Force, Sept. 2014.

[162] J. Peterson, H. Schulzrinne, and H. Tschofenig, "Secure telephone identity problem statement and requirements," Request for Comments 7340, Internet Engineering Task Force, Sept. 2014.

[163] H. Tschofenig, H. Schulzrinne, and B. Aboba, "Trustworthy location," Request for Comments 7378, Internet Engineering Task Force, Dec. 2014.

[164] H. Schulzrinne, S. McCann, G. Bajko, H. Tschofenig, and D. Kroeselberg, "Extensions to the emergency services architecture for dealing with unauthenticated and unauthorized devices," Request for Comments 7406, Internet Engineering Task Force, Dec. 2014.

[165] H. Schulzrinne, A. Rao, R. Lanphier, M. Westerlund, and M. Stiemerling, "Real-time streaming protocol version 2.0," Request for Comments 7826, Internet Engineering Task Force, Dec. 2016.

[166] C. Jennings, B. Lowekamp, E. Rescorla, S. Baset, H. Schulzrinne, and T. Schmidt, "A SIP usage for REsource LOcation And Discovery (RELOAD)," Request for Comments 7904, Internet Engineering Task Force, Oct. 2016.

[167] H. Schulzrinne, "A SIP response code for unwanted calls," Request for Comments 8197, Internet Engineering Task Force, July 2017.

[1] H. Schulzrinne, "The Internet is a series of tubes," Technical Report cucs-027-14, Department of Computer Science, Columbia University, New York, New York, Nov. 2014.

[2] H. Nam, K.-H. Kim, D. Calin, and H. Schulzrinne, "Towards dynamic network condition-aware video server selection algorithms over wireless networks," Technical Report cucs-001-14, Department of Computer Science, Columbia University, New York, New York, Jan. 2014.

[3] H. Nam, K. H. Kim, B. H. Kim, D. Calin, and H. Schulzrinne, "Towards a dynamic QoS-aware over-the-top video streaming in LTE," Technical Report cucs-002-14, Department of Computer Science, Columbia University, New York, New York, Jan. 2014.

[4] A. Singh, G. Ormazabal, S. Addepalli, and H. Schulzrinne, "Heterogeneous access: Survey and design considerations," Technical Report cucs-028-13, Department of Computer Science, Columbia University, New York, New York, Oct. 2013.

[5] H. Nam, B. H. Kim, D. Calin, and H. Schulzrinne, "A mobile video traffic analysis: Badly designed video clients can waste network bandwidth," Technical Report cucs-018-13, Department of Computer Science, Columbia University, New York, New York, July 2013.

[6] H. Nam, J. Janak, and H. Schulzrinne, "Connecting the physical world with Arduino in SECE," Technical Report cucs-013-13, Department of Computer Science, Columbia University, New York, New York, May 2013.

[7] J. Marasevic, J. Janak, H. Schulzrinne, and G. Zussman, "WiMAX in the classroom: Designing a cellular networking hands-on lab," Technical Report 2013-03-14, Department of Electrical Engineering, Columbia University, New York, New York, Mar. 2013.

[8] W. Song, J. W. Lee, B. S. Lee, and H. Schulzrinne, "Finding 9-1-1 callers in tall buildings," Technical Report cucs-001-13, Columbia University, New York, New York, Jan. 2013.

[9] W. Song, J. W. Lee, B. S. Lee, and H. Schulzrinne, "Improving vertical accuracy of indoor positioning for emergency communication," Technical Report cucs-016-12, Columbia University, New York, New York, Oct. 2012.

[10] J. W. Lee, R. Francescangeli, W. Song, E. Maccherani, J. Janak, S. Srinivasan, M. S. Kester, S. A. Baset, and H. Schulzrinne, "NetServ: Reviving active networks," Technical Report cucs-001-12, Columbia University, New York, New York, Jan. 2012.

[11] J. Janak, J. W. Lee, and H. Schulzrinne, "GRAND: Git revisions as named data," Technical Report cucs-047-11, Columbia University, New York, New York, Dec. 2011.

[12] S. Srinivasan, J. W. Lee, D. Batni, and H. Schulzrinne, "ActiveCDN: Cloud computing meets content delivery networks," Technical Report cucs-045-11, Columbia University, New York, New York, Nov. 2011.

[13] E. Maccherani, J. W. Lee, M. Femminella, G. Reali, and H. Schulzrinne, "NetServ on OpenFlow 1.0," Technical Report cucs-036-11, Columbia University, New York, New York, Sept. 2011.

[14] S. Seo, J. Janak, and H. Schulzrinne, "Columbia University WiMAX campus deployment and installation," Technical Report cucs-032-11, Columbia University, New York, New York, June 2011.

[15] K. H. Kim, V. K. Singh, and H. Schulzrinne, "DYSWIS: collaborative network fault diagnosis - of end-users, by end-users, for end-users," Tech. Rep. cucs-017-11, Columbia University, May 2011.

[16] J. W. Lee, R. Francescangeli, W. Song, J. Janak, S. Srinivasan, M. Kester, S. A. Baset, E. Liu, H. Schulzrinne, V. Hilt, Z. Despotovic, and W. Kellerer, "NetServ framework design and implementation 1.0," Tech. Rep. cucs-016-11, Columbia University, May 2011.

[17] A. Srivastava, J. W. Lee, and H. Schulzrinne, "Implementing zeroconf in linphone," Tech. Rep. cucs-011-11, Columbia University, Mar. 2011.

[18] M. Kester, E. Liu, J. W. Lee, and H. Schulzrinne, "NetServ: early prototype experiences," Tech. Rep. cucs-031-10, Columbia University, Dec. 2010.

[19] H. Cui, S. Srinivasan, and H. Schulzrinne, "ONEChat: enabling group chat and messaging in opportunistic networks," Tech. Rep. cucs-001-10, Columbia University, Jan. 2010.

[20] S. G. Hong, H. Schulzrinne, and S. Weiland, "PBS: signaling architecture for network traffic authorization," Tech. Rep. cucs-045-09, Columbia University, Oct. 2009.

[21] C. Shen and H. Schulzrinne, "On TCP-based SIP server overload control," Tech. Rep. cucs-048-09, Columbia University, Nov. 2009.

[22] C. Shen, E. Nahum, H. Schulzrinne, and C. Wright, "The impact of TLS on SIP server performance," Tech. Rep. cucs-022-09, Columbia University, May 2009.

[23] K. Ono and H. Schulzrinne, "Have i met you before? using Cross-Media relations to reduce SPIT," Tech. Rep. cucs-020-09, Columbia University, Apr. 2009.

[24] S.-G. Hong, S. Srinivasan, and H. Schulzrinne, "Measurements of multicast service discovery in a campus wireless network," Tech. Rep. cucs-050-08, Columbia University, Nov. 2008.

[25] S. Subramanya, X. Wu, and H. Schulzrinne, "VoIP-based air traffic controller training," Tech. Rep. cucs-043-08, Columbia University, Sept. 2008.

[26] S. Shin and H. Schulzrinne, "Towards the quality of service for VoIP traffic in IEEE 802.11 wireless networks," Tech. Rep. cucs-035-08, Columbia University, July 2008.

[27] C. Shen, H. Schulzrinne, and E. Nahum, "SIP server overload control: Design and evaluation," Tech. Rep. cucs-031-08, Columbia University, June 2008.

[28] A. Forte, S. Shin, and H. Schulzrinne, "IEEE 802.11 in the large: Observations at an IETF meeting," Tech. Rep. cucs-025-08, Columbia University, May 2008.

[29] E. Brosh, S. Baset, V. Misra, D. Rubenstein, and H. Schulzrinne, "The Delay-Friendliness of TCP," Tech. Rep. cucs-014-08, Columbia University, Mar. 2008.

[30] S. Abdul Baset, E. Brosh, V. Misra, D. Rubenstein, and H. Schulzrinne, "The Delay-Friendliness of TCP," Tech. Rep. cucs-023-07, Columbia University, June 2007.

[31] K. Ono and H. Schulzrinne, "The impact of SCTP on server scalability and performance," Tech. Rep. cucs-012-08, Columbia University, Feb. 2008.

[32] K. Ono and H. Schulzrinne, "One server per city: Using TCP for very large SIP servers," Tech. Rep. cucs-009-08, Columbia University, Feb. 2008.

[33] K. Arabshian, C. Dickmann, and H. Schulzrinne, "Service composition in a global service discovery system," Tech. Rep. cucs-033-07, Columbia University,, Sept. 2007.

[34] S. Hong, S. Srinivasan, and H. Schulzrinne, "Accelerating service discovery in Ad-Hoc zero configuration networking," Technical Report cucs-009-07, Columbia University, New York, Feb. 2007.

[35] A. Forte and H. Schulzrinne, "Cooperation between stations in wireless networks," arXiv report cs.NI/0701046, arXiv, Jan. 2007.

[36] K. Arabshian and H. Schulzrinne, "Combining ontology queries with text search in service discovery," Tech. Rep. cucs-006-07, Columbia University, New York, NY, Jan. 2007.

[37] O. Boyaci and H. Schulzrinne, "Measurements of DNS stability," Tech. Rep. cucs-045-06, Columbia University, New York, Dec. 2006.

[38] A. Forte, S. Shin, and H. Schulzrinne, "IEEE 802.11 in the large: Observations at an IETF meeting," tech. rep., Columbia University, Dec. 2006.

[39] A. Forte and H. Schulzrinne, "Cooperation between stations in wireless networks," Tech. Rep. cucs-044-06, Columbia University, New York, Dec. 2006.

[40] V. Singh, H. Schulzrinne, M. Isomaki, and P. Boni, "Presence traffic optimization techniques," Tech. Rep. cucs-041-06, Columbia University, New York, Nov. 2006.

[41] C. Shen and H. Schulzrinne, "A VoIP privacy mechanism and its application in VoIP peering for voice service provider topology and identity hiding," Tech. Rep. cucs-039-06, Columbia University, New York, Oct. 2006.

[42] S. Baset and H. Schulzrinne, "A common protocol for implementing various DHT algorithms," Tech. Rep. cucs-040-06, Columbia University, New York, Oct. 2006.

[43] C. Shen and H. Schulzrinne, "Measurement and evaluation of ENUM server performance," Tech. Rep. cucs-029-06, Columbia University, New York, Sept. 2006.

[44] S. Shin, A. Forte, and H. Schulzrinne, "Seamless layer-2 handoff using two radios in IEEE 802.11 wireless networks," Tech. Rep. cucs-018-06, Columbia University, Computer Science Department, Apr. 2006.

[45] A. Forte, S. Shin, and H. Schulzrinne, "Passive duplicate address detection for dynamic host configuration protocol (DHCP)," Tech. Rep. cucs-011-06, Columbia University, Computer Science Department, Mar. 2006.

[46] K. Singh and H. Schulzrinne, "Using an external DHT as a SIP location service," Technical Report CUCS-007-06, Columbia University, Computer Science Department, New York, NY, Feb. 2006.

[47] V. Singh and H. Schulzrinne, "A survey of security issues and solutions in presence," Tech. Rep. cucs-019-06, Columbia University, New York, Feb. 2006.

[48] V. Singh and H. Schulzrinne, "SIMPLEstone - benchmarking presence server performance," Tech. Rep. cucs-023-06, Columbia University, New York, Feb. 2006.

[49] M. Cristofano, A. Forte, and H. Schulzrinne, "Generic models for mobility management in next generation networks," Tech. Rep. cucs-031-05, Columbia University, Computer Science Department, Aug. 2005.

[50] K. Arabshian and H. Schulzrinne, "Hybrid hierarchical and Peer-to-Peer ontology-based global service discovery system," Tech. Rep. CUCS-016-05, Columbia University, Apr. 2005.

[51] C. Shen, H. Schulzrinne, S.-H. Lee, and J. Bang, "Internet routing dynamics and NSIS related considerations," Technical Report CUCS-007-05, Columbia University, New York, Feb. 2005.

[52] R. Shacham, H. Schulzrinne, S. Thakolsri, and W. Kellerer, "The virtual device: Expanding wireless communication services through service discovery and session mobility," Technical Report CUCS-001-05, Department of Computer Science, Columbia University, New York, NY, Jan. 2005.

[53] X. Wu and H. Schulzrinne, "End system service examples," Tech. Rep. CUCS-048-04, Columbia University Department of Computer Science, New York, New York, Dec. 2004.

[54] S. Baset and H. Schulzrinne, "An analysis of the Skype Peer-to-Peer internet telephony protocol," arXiv report cs.NI/0412017, arXiv, Dec. 2004. CUCS-039-04.

[55] K. Srivastava and H. Schulzrinne, "Preventing spam for SIP-based instant messages and sessions," Technical Report CUCS-042-04, Department of Computer Science, Columbia University, New York, NY, Oct. 2004.

[56] K. Singh and H. Schulzrinne, "Peer-to-Peer internet telephony using SIP," Tech. Rep. CUCS-044-04, Department of Computer Science, Columbia University, New York, NY, Oct. 2004.

[57] X. Wu and H. Schulzrinne, "Service learning in internet telephony," technical report, Department of Computer Science, Columbia University, Oct. 2004.

[58] X. Zhang and H. Schulzrinne, "Voice over TCP and UDP," Technical Report CUCS-033-04, Columbia University Department of Computer Science, Sept. 2004.

[59] K. Singh and H. Schulzrinne, "Failover and load sharing in SIP telephony," Tech. Rep. CUCS-011-04, Columbia University, Computer Science Department, New York, NY, USA, Mar. 2004.

[60] X. Wu and H. Schulzrinne, "Feature interactions in internet telephony end systems," tech. rep., Department of Computer Science, Columbia University, Jan. 2004.

[61] H. Schulzrinne, "9-1-1 calls for voice-over-ip," Ex-parte filing to the Federal Communications Commission cucs-022-03, Department of Computer Science, Columbia University, New York, New York, Aug. 2003.

[62] C. Wieser, M. Laakso, and H. Schulzrinne, "Security testing of SIP implementations," Technical Report CUCS-024-03, Department of Computer Science, Columbia University, New York, Aug. 2003.

[63] K. Singh, X. Wu, J. Lennox, and H. Schulzrinne, "Comprehensive multi-platform collaboration," Tech. Rep. CUCS-027-03, Dept. of Computer Science, Columbia University, New York, New York, Dec. 2003.

[64] K. Singh, W. Jiang, J. Lennox, S. Narayanan, and H. Schulzrinne, "CINEMA: columbia internet extensible multimedia architecture," technical report CUCS-011-02, Department of Computer Science, Columbia University, New York, New York, May 2002.

[65] H. Schulzrinne and K. Arabshian, "Providing emergency services in Internet telephony," technical report, Department of Computer Science, Columbia University, New York, NY, Apr. 2002.

[66] P. Mendes, H. Schulzrinne, and E. Monteiro, "Session-aware popularity-based resource allocation across several differentiated service domains," Technical Report CUCS-009-02, Columbia University, Apr. 2002.

[67] H. Schulzrinne, S. Narayanan, J. Lennox, and M. Doyle, "SIPstone - benchmarking SIP server performance," Technical Report CUCS-005-02, Department of Computer Science, Columbia University, New York, New York, Mar. 2002.

[68] W. Zhao and H. Schulzrinne, "A flexible and efficient protocol for multi-scope service registry replication," Tech. Rep. CUCS-016-02, Dept. of Computer Science, Columbia University, New York, New York, Mar. 2002.

[69] G. Camarillo, H. Schulzrinne, and R. Kantola, "Signalling transport protocols," Technical report CUCS-002-02, Dept. of Computer Science, Columbia University, New York, Feb. 2002.

[70] M. Papadopouli and H. Schulzrinne, "Performance of data dissemination and message relaying in mobile ad hoc networks," Technical Report CUCS-004-02, Dept. of Computer Science, Columbia University, New York, New York, Feb. 2002.

[71] S. Krishnan and H. Schulzrinne, "On buffered clos switches," Tech. Rep. CUCS-023-02, Dept. of Computer Science, Columbia University, New York, New York, Nov. 2002.

[72] P. Mendes, H. Schulzrinne, and E. Monteiro, "Multi-layer utilization maximal fairness for multi-rate multimedia sessions," Technical Report CUCS-008-01, Dept. of Computer Science, Columbia University, New York, New York, July 2001.

[73] M. Papadopouli and H. Schulzrinne, "Performance of data dissemination among mobile devices," technical report CUCS-005-01, Dept. of Computer Science, Columbia University, New York, New York, July 2001.

[74] P. Pan and H. Schulzrinne, "PF_IPOPTION: a kernel extension for IP option packet processing," Technical Memorandum 10009669-02TM, Bell Labs, Lucent Technologies, Murray Hill, NJ, June 2000.

[75] P. Pan and H. Schulzrinne, "Lightweight resource reservation signaling: Design, performance and implementation," Technical Memorandum 10009669-03TM, Bell Labs, Lucent Technologies, Murray Hill, NJ, June 2000.

[76] D. Rubenstein, J. Lennox, J. Rosenberg, and H. Schulzrinne, "Bell labs/columbia/umass RTP library internal function descriptions," Tech. Rep. 99-76, University of Massachusetts, Amherst, Massachusetts, Nov. 1999.

[77] W. Jiang and H. Schulzrinne, "QoS measurement of Internet real-time multimedia services," Technical Report CUCS-015-99, Columbia University, New York, New York, Dec. 1999.

[78] J. Rosenberg, J. Lennox, and H. Schulzrinne, "Programming Internet telephony services," Technical Report CUCS-010-99, Columbia University, New York, New York, Mar. 1999.

[79] J. Lennox, H. Schulzrinne, and T. L. Porta, "Implementing intelligent network services with the session initiation protocol," Technical Report CUCS-002-99, Columbia University, New York, New York, Jan. 1999.

[80] H. Schulzrinne and J. Rosenberg, "Signaling for Internet telephony," Technical Report CUCS-005-98, Columbia University, New York, New York, Feb. 1998.

[81] H. Schulzrinne, B. Deffner, D. Sisalem, and T. Friedman, "Architecture of a teleteaching application for testing resource reservation and adaptive applications in integrated networks," Project Report MMTng M-1, GMD Fokus, Berlin, Germany, Nov. 1995.

[82] I. Busse, B. Deffner, D. Cochrane, B. Gorman, H. Schulzrinne, P. Demestichas, Y. Manolessos, and K. Kassapakis, "Dynamic QoS management framework for IBC networks (D12)," Deliverable R2116/CRAY/WP2/DS/R/, RACE Project 2116 (TOMQAT), Nov. 1995.

[83] I. Busse, B. Deffner, H. Schulzrinne, P. Demestichas, Y. Manolessos, K. Kassapakis, G. D. Stamoulis, and G. Seehase, "TOMQAT test system user manual (D11)," Deliverable R2116/TELMAT/WP3/DS/, RACE Project 2116 (TOMQAT), Sept. 1995.

[84] I. Busse, B. Deffner, H. Schulzrinne, P. Demestichas, Y. Manolessos, K. Kassapakis, G. D. Stamoulis, and G. Seehase, "Preliminary test report and QoS verification document (D9)," Deliverable R2116/TUB/WP3/DS/P/0, RACE Project 2116 (TOMQAT), Aug. 1995.

[85] I. Busse, B. Deffner, H. Schulzrinne, P. Demestichas, Y. Manolessos, K. Kassapakis, G. D. Stamoulis, and G. Seehase, "Definition of conceptual framework for QoS management (D8)," Deliverable R2116/NTUA/WP2/DS/P/, RACE Project 2116 (TOMQAT), Feb. 1995.

[86] I. Busse, D. Cochrane, B. Deffner, P. Demestichas, B. Evans, W. Grupp, N. Karatzas, and K. Kassapakis, "Quality module specification (D7)," Deliverable R2116/ISR/WP2/DS/S/0, RACE Project 2116 (TOMQAT), Dec. 1994.

[87] H. Almus, H. Buschermoehle, I. Busse, B. Deffner, P. H. Georgatsos, W. Grupp, N. Karatzas, and K. Kassapaskis, "Architecture of the TOMQAT system and definition of net infrastructure (D6)," Deliverable R2116/TUB/WP2/DS/P/0, RACE Project 2116 (TOMQAT), Aug. 1994.

[88] D. Cochrane, P. Demestichas, A. Gehring, P. H. Georgatsos, J. Kawalek, N. Karatzas, K. Kassapakis, and P. Legand, "Requirement analysis and approach to dynamic total quality management (D5)," Deliverable R2116/ICOM/WP2/DS/P/, RACE Project 2116 (TOMQAT), Aug. 1994.

[89] A. Gehring, J. Kuwalek, P. Legand, Z. Lioupas, Y. Manolessos, K. Nagel, E. Papachristou, and I. Schieferdecker, "Requirement analysis and approach for dynamic total quality management (D4)," Deliverable R2116/ICOM/WP2/DSR/0, RACE Project 2116 (TOMQAT), June 1994.

[90] H. Almus, H. Buschermöhle, I. Busse, P. H. Georgatsos, W. Grupp, K. Kassapakis, P. Legand, and Z. Lioupas, "Architecture of the TOMQAT system and definition of net infrastructure (D3)," Deliverable R2116/GMD/WP2/DS/P/0, RACE Project 2116 (TOMQAT), May 1994.

[91] L. Kleinrock, J. P. Sterbenz, N. F. Maxemchuk, S. S. Lam, H. Schulzrinne, and P. Steenkiste, "The national exchange for networked information systems: a white paper," Technical Report CSD-930039, University of California (UCLA), Los Angeles, California, Nov. 1993.

[92] H. Schulzrinne, "Issues in designing a transport protocol for audio and video conferences and other multiparticipant real-time applications." expired Internet draft, Oct. 1993.

[93] A. M. Lapone, N. Maxemchuk, and H. Schulzrinne, "The bell laboratories network emulator," Technical Memorandum BL0113820-930913-64T, AT&T Bell Laboratories, Murray Hill, New Jersey, Sept. 1993.

[94] H. Schulzrinne, *Reducing and characterizing packet loss for high-speed computer networks with real-time services*. PhD thesis, University of Massachusetts, Amherst,

Massachusetts, May 1993. also: Technical Report 93-54, Department of Computer Science, University of Massachusetts at Amherst.

[95] H. Schulzrinne, J. F. Kurose, and D. F. Towsley, "Loss correlation for queues with single and multiple input streams," Technical Report TR 92-53, Department of Computer Science, University of Massachusetts, Amherst, Massachusetts, July 1992.

[96] H. Schulzrinne, "Voice communication across the internet: A network voice terminal," Technical Report TR 92-50, Dept. of Computer Science, University of Massachusetts, Amherst, Massachusetts, July 1992.

[97] H. Schulzrinne, J. F. Kurose, and D. F. Towsley, "Distribution of the loss period for some queues in continuous and discrete time," Technical Report TR 91-03, Department of Computer and Information Science, University of Massachusetts, Amherst, Massachusetts, July 1991.

[98] H. Schulzrinne, J. F. Kurose, and D. F. Towsley, "Congestion control for real-time traffic in high-speed networks," Technical Report TR 89-92, Department of Computer and Information Science, University of Massachusetts, Amherst, Massachusetts, Mar. 1991.

[99] H. Schulzrinne, "SIMUL simulation system manual." internal memorandum, Feb. 1989.

[100] H. Schulz-Rinne, "Multistage vector quantization for speech and image waveform coding; the DSP workbench: Distributed multiprocess system simulation," Master's thesis, University of Cincinnati, Cincinnati, Ohio, Aug. 1987.

MASTERS THESES SUPERVISED

[1] R. Bollow, "Video transmission using the available bit rate service," Master's thesis, Berlin University of Technology, Berlin, Germany, Jan. 1997.

[2] C. Zahl, "Aufbau und konfiguration von internet-multimedia-konferenzen über verbindungen niedriger bandbreite (setup and configuration of Internet multimedia conferences using low-bandwidth links)," Master's thesis, Berlin University of Technology, Berlin, Germany, Feb. 1997. Diplomarbeit.

[3] F. Oertel, "Integration von ISDN-Teilnehmern in internet-multimedia-konferenzen (integration of ISDN subscribers into Internet multimedia conferences)," Master's thesis, Berlin University of Technology, Berlin, Germany, Feb. 1997. Diplomarbeit.

[4] C. Zahl, "Entwicklung einer internet-multimedia-telekommunikations-anlage (development of an Internet multimedia telecommunications system)," Studienarbeit, Department of Communication Networks, TU Berlin, Berlin, Germany, Nov. 1995.

[5] F. Oertel, "Aufbau und konfiguration lokaler multimedia konferenz-umgebungen (setup and configuration of local multimedia conferencing environments)," Studienarbeit, Department of Communication Networks, TU Berlin, Berlin, Germany, Nov. 1995.

[6] C. Sieckmeyer, "Bewertung von adaptiven ausspielalgorithmen für paketvermittelte audiodaten (evaluation of adaptive playout algorithms for packet audio)," Studienarbeit, Dept. of Electrical Engineering, TU Berlin, Berlin, Germany, Oct. 1995.

[7] B. Rathke, "Evaluation of a distance-vector based multicast-routing protocol for datagram internetworks," Diplomarbeit, Department of Telecommunications, TU Berlin, Berlin, Germany, Oct. 1995.

[8] I. Demirel, "Eine SDL-Spezifikation des core based tree (CBT) multicast-routing-protokolls (an SDL specification of the core-based tree (CBT) multicast routing protocol)," Studienarbeit, Dept. of Electrical Engineering, TU Berlin, Berlin, Germany, Sept. 1995.

[9] D. Sisalem, "Rate based congestion control and its effects on TCP over ATM," Diplomarbeit, School of Engineering, TU Berlin, Berlin, June 1995.

[10] S. Portner, "Verbindungsverwaltung in hochgeschwindigkeitsnetzen (connection management in high speed networks)," Studienarbeit, Institut für Fernmeldetechnik, TU Berlin, Berlin, Germany, Dec. 1994.

PHD THESES SUPERVISED

Jonathan Rosenberg, Xin Wang, Maria Papadopouli, Ping Pan, Wenyu Jiang, Lisa Amini, Jonathan Lennox, Kundan Singh, Santosh Krishnan, Weibin Zhao (2006), Xiaotao Wu (2007), Sangho Shin (2008), Knarig Arabshian (2008), Charles Shen (2010), Ashutosh Dutta (2010), Salman Baset (2010), Omer Boyaci (2011), Se Gi Hong (2011), Arezu Moghadam (2011), Jae Woo Lee (2012), Kumiko Ono (2012), Wonsang Song (2014), Jong Yul Kim (2015), Hyunwoo Nam (2015), Suman Srinivasan (2016), Kyung-Hwa Kim (2017).

CURRENT PHD STUDENTS

Jan Janak.

NON-US THESIS COMMITTEES

Ralf Ackermann (Technische Universität Darmstadt, July 2003), Paulo Mendes (University of Coimbra, Portugal, January 2004), Cristian Hesselman (University of Twente, Holland, May 2005), Martin Krebs (RWTH Aachen University, May 2010), Ian Marsh (KTH, Sweden, June 2009), Tommy Ou (University of Oulu, Finland, August 2010), Antti Mäkelä (Aalto University, Finland, August 2012), Erkki Harjula (University of Oulu, Finland, June 2016).

November 10, 2018

DECLARATION OF DR. HENNING G. SCHULZRINNE
***WIKIMEDIA FOUND. V. NSA*, NO. 1:15-CV-00662-TSE (D. MD.)**

EXHIBIT B

DOCUMENTS PROVIDED BY DEPARTMENT OF JUSTICE
FOR CONSIDERATION IN PREPARATION OF DECLARATION

1. NSA Director of Civil Liberties and Privacy Office Report, NSA's Implementation of FISA Section 702 (Apr. 16, 2014), https://www.nsa.gov/Portals/70/documents/about/civil-liberties/reports/nsa_report_on_section_702_program.pdf.

2. Privacy & Civil Liberties Oversight Board Report on the Surveillance Program Operated Pursuant to Section 702 of the FISA (July 2, 2014), https://www.pclob.gov/library/702-Report.pdf

3. Office of the Director of National Intelligence, Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (June 8, 2013), https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2013/item/871-facts-on-the-collection-of-intelligence-pursuant-to-section-702-of-the-foreign-intelligence-surveillance-act

4. The National Security Agency: Missions, Authorities, Oversight and Partnerships (Aug. 9, 2013), https://fas.org/irp/nsa/nsa-story.pdf

5. The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act (attachment to https://www.dni.gov/files/documents/Ltr%20to%20HPSCI%20Chairman%20Rogers%20and%20Ranking%20Member%20Ruppersberger_Scan.pdf)

6. *Wikimedia Found. v. NSA*, 143 F. Supp. 3d 344 (D. Md. 2015)

7. *Wikimedia Found. v. NSA*, 857 F.3d 193 (4th Cir. 2017)

8. Declaration of Robert T. Lee, ECF No. 77-3, *Wikimedia Found. v. NSA*, No. 1:15-cv-00662-TSE (D. Md.)

9. [*Redacted Caption*], Memorandum Opinion and Order (F.I.S.C. Apr. 26, 2017) (public redacted version), https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf

10. [*Redacted Caption*], 2011 WL 10945618 (F.I.S.C. Oct. 3, 2011) (public redacted version)

11. Wikimedia Foundation Inc.'s Responses and Objections to National Security Agency's First Set of Interrogatories (Jan. 11, 2018)

12. Wikimedia Foundation Inc.'s Responses and Objections to United States Department of Justice's First Set of Interrogatories (Jan. 11, 2018)

13. Wikimedia Foundation Inc.'s Responses and Objections to the Office of the Director of National Intelligence's First Set of Interrogatories (Jan. 11, 2018)

14. Documents produced in discovery by Plaintiff Wikimedia Foundation, beginning with Bates-stamp nos.: WIKI0001412, 1458, 1474, 1545, 1950, 1956, 1957, 1960, 2097, 2301, 2316, 2344, 2358, 2429, 2459, 2479, 2483, 5174, 5466, 5500, 5577, 5693, 5832, 5978, 6363, 6505, 6508, 6536, 6543, 6564, 6662, 6700, 6836, 6872, 7093, 7108, 7115, 7347, 7351, 7382, 8108, 9269

15. Exhibit 1 to Wikimedia Foundation, Inc.'s Amended Responses and Objections to Office of the Director of National Intelligence's Interrogatory No. 19 (Apr. 6, 2018), and Exhibits A-G thereto

16. Deposition of Michelle S. Paulson (Apr. 13, 2018)

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, Plaintiff, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	Civil Action No. 1:15-cv-00662-TSE

Attachment D

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, Plaintiff, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	Civil Action No. 1:15-cv-00662-TSE [redacted]

EXHIBIT 2

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, Plaintiff, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	No. 1:15-cv-0662 (TSE) [redacted]

Declaration of James J. Gilligan

Pursuant to 28 U.S.C. § 1746, I, James J. Gilligan, hereby declare:

1. I am an attorney in the United States Department of Justice, Civil Division, Federal Programs Branch. I serve as lead counsel for the Government Defendants in the above-captioned case. The statements made herein are based on my personal knowledge, and on information made available to me in the course of my duties and responsibilities as Government counsel in this case.

2. I submit this declaration in support of the Defendants' concurrently-filed motion for summary judgment.

3. Filed as Exhibits 3-5 attached to the Defendants' motion for summary judgment are true and correct copies of the following documents:

Exhibit No.	Exhibit Name
3	Wikimedia Foundation, Inc.'s Amended and Supplemental Responses and Objections to NSA's First Set of Interrogatories, dated March 23, 2018
4	Wikimedia Foundation, Inc.'s Amended Responses and Objections to ODNI's Interrogatory No. 19, dated April 6, 2018, including Exhibit 1, "Technical Statistics Chart"
5	Wikimedia Foundation, Inc.'s Responses and Objections to NSA's First Set of Interrogatories, dated January 11, 2018

I declare under penalty of perjury that the foregoing is true and correct. Executed in Washington, D.C., this 13th day of November, 2018.

JAMES J. GILLIGAN
Special Litigation Counsel
United States Department of Justice
Civil Division, Federal Programs Branch

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, Plaintiff, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	Civil Action No. 1:15-cv-00662-TSE

Attachment E

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, Plaintiff, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	Civil Action No. 1:15-cv-00662-TSE ~~FILED UNDER SEAL~~

EXHIBIT 3

IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, INC. Plaintiff, v. NATIONAL SECURITY AGENCY, et al., Defendants.	Civil Action No. 1:15-cv-00662-TSE Hon. T.S. Ellis, III

WIKIMEDIA FOUNDATION, INC.'S AMENDED AND SUPPLEMENTAL RESPONSES AND OBJECTIONS TO NATIONAL SECURITY AGENCY'S FIRST SET OF INTERROGATORIES

PROPOUNDING PARTY: NATIONAL SECURITY AGENCY

RESPONDING PARTY: WIKIMEDIA FOUNDATION, INC.

SET NUMBER: ONE

Pursuant to Federal Rule of Civil Procedure 33, Plaintiff Wikimedia Foundation, Inc. ("Plaintiff" or "Wikimedia") amends and supplements its responses as follows to Defendant National Security Agency's ("Defendant" or "NSA") (collectively with Plaintiff, the "Parties") First Set of Interrogatories (the "Interrogatories"):

I. GENERAL RESPONSES.

1. Plaintiff's response to Defendant's Interrogatories is made to the best of Plaintiff's present knowledge, information, and belief. Discovery in this action is ongoing, and Plaintiff's responses may be substantially altered by further investigation, including further review of Plaintiff's own documents, as well as the review of documents produced by Defendant. Said response is at all times subject to such additional or different information that discovery or

further investigation may disclose and, while based on the present state of Plaintiff's recollection, is subject to such refreshing of recollection, and such additional knowledge of facts, as may result from Plaintiff's further discovery or investigation.

2. Plaintiff reserves the right to make any use of, or to introduce at any hearing and at trial, information and/or documents responsive to Defendant's Interrogatories but discovered subsequent to the date of this response, including, but not limited to, any such information or documents obtained in discovery herein.

3. To the extent that Plaintiff responds to Defendant's Interrogatories by stating that Plaintiff will provide information and/or documents that Plaintiff deems to embody material that is private, business confidential, proprietary, trade secret, or otherwise protected from disclosure pursuant to Federal Rule of Civil Procedure 26(c)(7), Federal Rule of Evidence 501, or other applicable law, Plaintiff will do so only pursuant to the Parties' Stipulated Protective Order (ECF No. 120).

4. Plaintiff reserves all objections or other questions as to the competency, relevance, materiality, privilege, or admissibility as evidence in any subsequent proceeding in or trial of this or any other action for any purpose whatsoever of Plaintiff's responses herein and any document or thing identified or provided in response to Defendant's Interrogatories.

5. Plaintiff's responses will be subject to and limited by any agreements the Parties reach concerning the scope of discovery.

6. Plaintiff reserves the right to object on any ground at any time to such other or supplemental interrogatories as Defendant may at any time propound involving or relating to the subject matter of these Interrogatories.

II. GENERAL OBJECTIONS.

Plaintiff makes the following general objections, whether or not separately set forth in response to each Interrogatory, to each instruction, definition, and Interrogatory made in Defendant's Interrogatories:

1. Plaintiff objects to the Interrogatories in their entirety insofar as any such instruction, definition, or Interrogatory seeks information or production of documents protected by the attorney-client privilege or the work product doctrine. Fed. R. Civ. Proc. 26(b)(1). Such information or documents shall not be provided in response to Defendant's Interrogatories and any inadvertent disclosure or production thereof shall not be deemed a waiver of any privilege with respect to such information or documents or of any work product immunity which may attach thereto. Fed. R. Civ. Proc. 26(b)(5)(B).

2. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory seeks identification of documents, witnesses, or information that Defendant has withheld from Plaintiff. Fed. R. Civ. Proc. 26(b)(1), (2).

3. Plaintiff objects to the Interrogatories in their entirety to the extent any such Interrogatory requires Plaintiff to identify potentially thousands of pages of documents, not all of which have been or can be located and reviewed by counsel within the time period allowed for this response or within a reasonable time. Accordingly, said Interrogatories would subject Plaintiff to unreasonable and undue annoyance, oppression, burden and expense.

4. Plaintiff objects to any Interrogatories that exceed the scope of jurisdictional discovery as defined by Defendants, *see* ECF No. 116 at 4, and ordered by the Court.

5. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory seeks information that is available through or from public

sources or records, or that are otherwise equally available to Defendant, on the ground that such instructions, definitions, and/or Interrogatories unreasonably subject Plaintiff to undue annoyance, oppression, burden, and expense. Fed. R. Civ. Proc. 26(b)(1), (2).

6. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory purport to impose obligations that are greater or more burdensome than or contradict those imposed by the applicable Federal and local rules. *See* Fed. R. Civ. Proc. 26, 33.

7. Plaintiff objects to the Interrogatories in their entirety as the Interrogatories contain more than the "25 written interrogatories, including all discrete subparts," permitted by the Federal Rules of Civil Procedure, Rule 33(a)(1), and Defendant has not sought leave to serve additional interrogatories.

8. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory seeks documents or information no longer in existence or not currently in Plaintiff's possession, custody, or control, or to the extent they refer to persons, entities, or events not known to Plaintiff or controlled by Plaintiff, on the grounds that such definitions or Interrogatories are overly broad, seek to require more of Plaintiff than any obligation imposed by law, would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense, and would seek to impose upon Plaintiff an obligation to investigate, discover, or produce information or materials from third parties or otherwise that are accessible to Defendant or readily obtainable from public or other sources. Fed. R. Civ. Proc. 26(b)(1), (2).

9. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory seeks information or production of documents protected

from disclosure by any right to privacy or any other applicable privilege or protection, including the right to confidentiality or privacy of third parties, any right of confidentiality provided for by Plaintiff's contracts or agreements with such third parties, or by Plaintiff's obligations under applicable law or contract to protect such confidential information. Plaintiff reserves the right to withhold any responsive information or documents governed by a third-party confidentiality agreement until such time as the appropriate notice can be given or the appropriate permissions can be obtained. Plaintiff also objects generally to all instructions, definitions, or Interrogatories to the extent they seek disclosure of trade secrets and other confidential research or analyses, development, or commercial information of Plaintiff or any third party.

10. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory is overbroad and unduly burdensome, particularly to the extent they seek "all," "each," or "any" documents, witnesses or facts relating to various subject matters. Fed. R. Civ. Proc. 26(b)(1), (2). To the extent Plaintiff responds to such Interrogatories, Plaintiff will use reasonable diligence to identify responsive documents, witnesses or facts in its possession, custody, or control, based on its present knowledge, information, and belief.

11. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory seeks expert discovery prematurely.

12. Plaintiff objects to any contention Interrogatories in their entirety as premature. Plaintiff will provide its response prior to the close of fact discovery.

13. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory purports to require Plaintiff to restore and/or search data sources that are not reasonably accessible on the grounds that such definitions and Interrogatories would subject Plaintiff to undue burden and expense. Fed. R. Civ. Proc. 26(b)(1), (2).

III. DEFINITIONAL OBJECTIONS.

1. Plaintiff objects to definition number one (1) to the extent it defines "Plaintiff" and "Wikimedia" to include Plaintiff's "parent, subsidiary, and affiliated organizations, and all persons acting on their behalf, including officials, agents, employees, attorneys, and consultants." Said definition is overly broad, seeks irrelevant information not calculated to lead to the discovery of admissible evidence, seeks information outside of Plaintiff's possession, custody, or control, and would subject Plaintiff to unreasonable and undue annoyance, oppression, burden and expense. Said definition is also vague and ambiguous in that it cannot be determined what is meant by the terms "affiliated organizations" and "all persons acting on their behalf." Plaintiff shall construe "Plaintiff" and "Wikimedia" to mean Wikimedia, and its present officers, directors, agents, and employees.

2. Plaintiff objects to definition number four (4) and to each Interrogatory that purports to require Plaintiff to "state the basis of," "stating the basis of," "state on what basis," or otherwise "state with particularity" or "identify" "all" facts, documents, or persons whose testimony support or dispute any given factual assertion, on the ground that any response thereto would require subjective judgment on the part of Plaintiff and its attorneys, and would further require disclosure of a conclusion or opinion of counsel in violation of the attorney work product doctrine and/or attorney-client privilege. Plaintiff further objects that this definition and all requests to identify documents in the Interrogatories are premature at this early stage of the litigation, would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense, and would impose an obligation to provide information greater than that required by the Federal Rules of Civil Procedure.

3. Plaintiff objects to definition number five (5) as unduly burdensome in that it

purports to require Plaintiff to "identify" each "natural person" by providing information including "her most current home and business addresses, telephone numbers, and e-mail addresses, the name of her current employer, and her title."

4. Plaintiff objects to definition number six (6) as unduly burdensome in that it purports to require Plaintiff to "identify" an "entity that is not a natural person" by providing information including "its telephone number and e-mail address, and the full names, business addresses, telephone numbers, and e-mail addresses of both its chief executive officer and an agent designated by it to receive service of process."

5. Plaintiff objects to definition number seven (7) as unduly burdensome in that it purports to require Plaintiff to "identify" documents by providing "(a) the nature of the document (*i.e.*, letter, memorandum, spreadsheet, database, etc.); (b) its date; (c) its author(s) (including title(s) or position(s)); (d) its recipient(s) (including title(s) or position(s)); (e) its number of pages or size; and (f) its subject matter," or by providing information in accordance with Defendant's "Specifications for Production of ESI and Digitized ('Scanned') Images attached to Defendant National Security Agency's First Set of Requests for Production." Plaintiff further objects that this definition and all requests to identify documents in the Interrogatories are premature at this early stage of the litigation, would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense, and would impose an obligation to provide information greater than that required by the Federal Rules of Civil Procedure.

IV. INSTRUCTIONAL OBJECTIONS

1. Plaintiff objects to instruction number one (1) to the extent it purports to request "knowledge or information" from Wikimedia's "parent, subsidiary, or affiliated organizations, and their officials, agents, employees, attorneys, consultants, and any other person acting on their

behalf." Said request is overly broad, seeks irrelevant information not calculated to lead to the discovery of admissible evidence, seeks information outside Plaintiff's possession, custody, or control, and would subject Plaintiff to unreasonable and undue annoyance, oppression, burden and expense. Moreover, said request is vague and ambiguous in that it cannot be determined what is meant by the term "affiliated organizations" and "any other person acting on their behalf." Where an Interrogatory requests knowledge or information of Plaintiff, Plaintiff shall construe such request to mean knowledge or information from Wikimedia, and its present officers, directors, agents, and employees.

2. Plaintiff objects to instruction number three (3) as unduly burdensome and imposing an obligation to provide information greater than that required by the Federal Rules of Civil Procedure to the extent it purports to require Plaintiff to "identify each person known by Plaintiff to have such knowledge, and in each instance where Plaintiff avers insufficient knowledge or information as a grounds for not providing information or for providing only a portion of the information requested, set forth a description of the efforts made to locate information needed to answer the interrogatory."

3. Plaintiff objects to instruction number four (4) to the extent it seeks to require it to identify anything other than the specific claim of privilege or work product being made and the basis for such claim, and to the extent it seeks to require any information not specified in Discovery Guideline 10, on the grounds that the additional information sought by Defendant would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense, and constitutes information protected from discovery by privilege and as work product. Plaintiff is willing to discuss acceptable reciprocal obligations for disclosure of information withheld on the basis of attorney-client privilege or attorney work-product.

4. Plaintiff objects to instruction number five (5) to the extent it defines "the time period for which each interrogatory seeks a response" as "the period from July 10, 2008 (the date of enactment of the FISA Amendments Act of 2008, Pub. L. 110-261, 121 Stat. 522) until the date of Plaintiff's response." This definition is overly broad, seeks irrelevant information not calculated to lead to the discovery of admissible evidence, and would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense. Where appropriate, Plaintiff has defined the specific time period encompassed by specific responses.

5. Plaintiff objects to instruction number six (6) that the Interrogatories are continuing, to the extent said instruction seeks unilaterally to impose an obligation to provide supplemental information greater than that required by Federal Rule of Civil Procedure 26(e) and would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense. Plaintiff will comply with the requirements of the Federal Rules of Civil Procedure and is willing to discuss mutually acceptable reciprocal obligations for continuing discovery.

V. SPECIFIC OBJECTIONS AND RESPONSES TO INTERROGATORIES.

Without waiving or limiting in any manner any of the foregoing General Objections, Definitional Objections, or Instructional Objections, but rather incorporating them into each of the following responses to the extent applicable, Plaintiff responds to the specific Interrogatories in Defendant's Interrogatories as follows:

INTERROGATORY NO. 2:

Unless Plaintiff's response to Interrogatory No. 1, above, is an unequivocal "no," then please state the basis of Plaintiff's contention that NSA Upstream surveillance involves the interception, copying, and review of all or substantially all international Internet text-based communications, including, but not limited to, the contentions that "Upstream surveillance is

intended to enable the comprehensive monitoring of international internet traffic," see Amended Complaint ¶ 48; that "the NSA is temporarily copying and then sifting through the contents of what is apparently most e mails and other text-based communications that cross the border," see id. ¶ 69; that "it would be difficult to systematically search the contents of the communications without first gathering nearly all cross-border text-based data," see Pl.'s Opp. to Defs.' MTD at 18-19; and that the U.S. Government "has acknowledged ... that the NSA ... examines the full contents of essentially everyone's communications to determine whether they include references to the NSA's search terms," *see id.* at 10.

RESPONSE TO INTERROGATORY NO. 2:

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory is a contention Interrogatory that is premature at this stage in the litigation. Plaintiff further submits that these matters may be the subject of expert testimony, as to which Plaintiff will provide discovery at the appropriate time.

Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery. Plaintiff additionally objects that this Interrogatory is improperly compound in that it contains multiple subparts.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

The bases for Plaintiff's contention include the following:

- Basic principles underlying how Internet communications are transmitted and how surveillance on a packet-switched network operates.

- Privacy & Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of FISA* (2014) ("PCLOB Report"), including pages 7–10, 12–

13, 22, 30–41 & n.157, 79, 111 n.476, 120–22, 125, 143, and official government sources concerning Upstream surveillance cited therein.

- [*Redacted*], No. [Redacted], 2011 WL 10945618 (FISC Oct. 3, 2011)
- 50 U.S.C. §§ 1801, 1881a.
- David S. Kris & J. Douglas Wilson, *National Security Investigations and Prosecutions* § 17.5 (July 2015)
- Julia Angwin & Jeff Larson, *New Snowden Documents Reveal Secret Memos Expanding Spying*, ProPublica (June 4, 2015) (and associated documents)
- Julia Angwin et al., *AT&T Helped U.S. Spy on Internet on Vast Scale*, N.Y. Times, Aug. 15, 2015 (and associated documents)
- Julia Angwin et al., *NSA Spying Relies on AT&T's 'Extreme Willingness to Help'*, ProPublica, Aug. 15, 2015 (and associated documents)
- Jeff Larson et al., *A Trail of Evidence Leading to AT&T's Partnership with the NSA*, ProPublica, Aug. 15, 2015 (and associated documents)
- PCLOB, Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 26:15–18 (Mar. 19, 2014) (statement of Robert Litt, General Counsel, ODNI)
- Charlie Savage, *Power Wars* (2015)

Additionally, Plaintiff's contention is based on the principles of Internet communication and the technical necessities of the inspection of Internet communications in transit.

For example, Internet communications in transit are split into packets. Where an eavesdropper is attempting to determine whether the contents of a particular communication in transit on the Internet contain a particular piece of information, the eavesdropper generally must

reassemble the packets constituting the communication and then scan the reassembled communication. Reassembling Internet packets requires the temporary copying (or "caching") of those packets until all packets needed for the reassembly have arrived.

Additionally, Upstream surveillance involves the retention of communications that contain targeted selectors. To retain a communication in transit, an eavesdropper must copy and reassemble the packets constituting the communication. But because an eavesdropper cannot know in advance which packets in transit are part of a communication containing a targeted selector, the eavesdropper must create a temporary copy of all packets that might be a part of such a communication.

The fact that all or substantially all international Internet text-based communications are subject to Upstream surveillance follows necessarily from the information the government has officially disclosed, and it is corroborated by independent news reports. For Upstream surveillance to serve the purposes the government has said it serves, the NSA must be comprehensively monitoring text-based communications originating or terminating in the United States. This is the only way for the NSA to reliably obtain communications to, from, and about its thousands of targets around the world, because those communications travel along paths in and out of the country that are unpredictable and change over time. Moreover, the structure of the Internet backbone facilitates such comprehensive surveillance. Because international communications are channeled through a small number of Internet chokepoints—and because the NSA's own documents show that it is conducting Upstream surveillance at many of those chokepoints—it is straightforward for the government to conduct the comprehensive surveillance necessary for Upstream to function as described.

The government's descriptions of Upstream surveillance make clear that the government

is interested in obtaining, with a high degree of confidence, all international communications to, from, and about its targets. For example, the Privacy and Civil Liberties Oversight Board has described the use of Upstream surveillance to collect "about" communications as "an inevitable byproduct of the government's efforts to *comprehensively* acquire communications that are sent to or from its targets." PCLOB Report 10 (emphasis added). And it has said about Upstream surveillance more generally that this method's "success . . . depends on collection devices that can reliably acquire data packets associated with the proper communications." *Id.* at 143 (emphasis added).

Because the routing of Internet traffic is unpredictable, however, the government can only "comprehensively" and "reliably" obtain communications to, from, and about its thousands of targets by conducting its surveillance on the different routes by which Internet communications enter and leave the country, and by examining substantially all international communications that travel those various routes.

The path that an Internet communication takes is inherently unpredictable. Internet communications are routed around the globe based on a complex set of rules and relationships that are applied dynamically, based on network conditions at any given moment. These network conditions change frequently, and so one cannot know in advance which path a particular communication will travel. Indeed, even the communications between two individuals in a single conversation (such as an Internet chat or email exchange) may take entirely different routes across the Internet backbone, even though the end-points are the same. For example, if an NSA target is having an Internet chat conversation with someone in the United States, the communications *from* the target will frequently follow a different path than those *to* the target. And, of course, a target's location may vary over time. For all these reasons, a target's

communications may traverse one Internet circuit at one moment, but a different one later.

The fact that the NSA had, at last public count, 106,469 surveillance targets (some of which are groups with perhaps hundreds or even thousands of members) only reinforces the conclusion that Upstream surveillance of international text-based communications must be comprehensive. *See* ODNI, Statistical Transparency Report Regarding the Use of National Security Authorities for Calendar Year 2016 (Apr. 2017), https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2016. The communications of so many targets scattered around the world will travel many different routes across the Internet backbone, based on the locations of those various targets, their individual movements over time, and changes in network conditions. These communications will be intermingled with those of the general population in the flow of Internet traffic. An intelligence agency that seeks to reliably intercept communications to, from, or about its targets, could do so only by searching substantially all text-based communications entering or leaving the country.

This allegation is based on the government's official disclosures and on necessary inferences from those disclosures, but it is also corroborated by news accounts. A *New York Times* report from August 2013 states, based on a review of NSA documents and interviews with senior intelligence officials, that "the N.S.A. is temporarily copying and then sifting through the contents of what is apparently most e-mails and other text-based communications that cross the border." Charlie Savage, *N.S.A. Said to Search Content of Messages to and from U.S.*, N.Y. Times, Aug. 8, 2013, http://nyti.ms/1E1nlsi. The same *New York Times* report also explains why the NSA's Upstream surveillance is so far-reaching:

> "Computer scientists said that it would be difficult to systematically search the contents of the communications without first gathering nearly all cross-border text-based data;

> fiber-optic networks work by breaking messages into tiny packets that flow at the speed of light over different pathways to their shared destination, so they would need to be captured and reassembled."

Id.; *see also* Charlie Savage, *Power Wars* 207–11 (2015).

Not only does the NSA have an overriding incentive to copy and review substantially all international Internet communications, but the Internet backbone is structured in a way that enables it to do so.

The Internet backbone funnels almost all Internet communications entering and leaving the country through a limited number of chokepoints. The Internet backbone includes a relatively small number of international submarine cables (and a limited number of terrestrial cables) that transport Internet traffic into and out of the United States. Because there are relatively few high-capacity cables carrying international Internet communications, there are correspondingly few chokepoints—*i.e.*, junctions through which all international Internet communications must pass en route to their destinations. By installing its surveillance equipment at the small number of backbone chokepoints, the NSA is able to monitor substantially all text-based communications entering or leaving the United States. And the government has acknowledged that it conducts Upstream surveillance at international links and on the Internet backbone. [*Redacted*], 2011 WL 10945618, at *15; PCLOB Report 36–37.

NSA documents published in the press show that the NSA has installed surveillance equipment at many major chokepoints on the Internet backbone. One of these NSA documents states that the NSA has established interception capabilities on "many of the chokepoints operated by U.S. providers through which international communications enter and leave the United States." *See* Plaintiff's First Amended Complaint ¶ 69. Another shows that just one of

those participating providers has facilitated Upstream surveillance at seven major international chokepoints in the United States. *Id.* ¶ 68. Additional reporting states that the NSA has installed surveillance equipment in at least 17 "internet hubs" operated by another major U.S. telecommunications provider. Julia Angwin et al., *NSA Spying Relies on AT&T's 'Extreme Willingness to Help'*, ProPublica, Aug. 15, 2015 (and associated documents).

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 2:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement as discovery in this case continues, Plaintiff supplements its response as follows:

The bases for Plaintiff's contention also include the following: Glenn Greenwald, *No Place to Hide* (2014).

The fact that the NSA had, at last public count, 106,469 surveillance targets (some of which are groups with perhaps hundreds or even thousands of members) only reinforces the conclusion that Upstream surveillance of international text-based communications must be comprehensive. *See* ODNI, Statistical Transparency Report Regarding the Use of National Security Authorities for Calendar Year 2016 (Apr. 2017), https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2016; *see generally* ODNI Statistical Transparency Reports Regarding the Use of National Security Authorities.

INTERROGATORY NO. 3:

Please identify each category of Wikimedia international, text-based, Internet communications that Plaintiff contends, for purposes of establishing jurisdiction, is intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance, including but not limited to, user visits to Wikimedia sites; contributions and edits to Wikimedia websites;

Wikimedia discussion forums; Wikimedia discussion pages; e mail sent via Wikimedia among registered users; communications "over wikis" among small or limited groups of users; mailing lists with restricted membership; other use of Wikimedia Projects, websites, and webpages by "community members" to interact with one another; internal log communications; "Community Consultations;" solicitations of user input and preferences; and other communications sent and received by Wikimedia staff in carrying out Wikimedia's work. *See* Amended Complaint ¶¶ 79, 84, 86, 92, 93, 102.

RESPONSE TO INTERROGATORY NO. 3:

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory seeks information that exceeds the scope of jurisdictional discovery as defined by Defendants, *see* ECF No. 116 at 4, and as ordered by the Court.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows. As explained in Wikimedia's First Amended Complaint, Wikimedia contends that Upstream surveillance implicates at least three categories of communications (Am. Compl. ¶ 86): (1) Wikimedia communications with its community members, who read and contribute to Wikimedia's Projects and webpages, and who use the Projects and webpages to interact with each other. Examples of these communications include, but are not limited to, page views to Wikimedia websites, edits and contributions to Wikimedia websites, emails between registered Wikimedia users and emails on Wikimedia's mailing lists.

(2) Wikimedia's internal log communications.

(3) Electronic communications of Wikimedia staff. Examples of these communications include, but are not limited to, Gmail, Google chat, Internet Relay Chat, and Slack. Additionally, Wikimedia staff members use a variety of third-party tools to conduct their work, including, but

not limited to, Google Apps/G Suite, Trello, Sugar, Qualtrics, User Testing and Salesforce.

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 3:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement as discovery in this case continues, Plaintiff supplements its response as follows:

As stated above, Wikimedia contends that Upstream surveillance implicates at least three categories of communications (Am. Compl. ¶ 86). The first category involves Wikimedia communications with its community members, who read and contribute to Wikimedia's Projects and webpages, and who use the Projects and webpages to interact with each other. Examples of these communications include, but are not limited to, page views to Wikimedia websites, edits and contributions to Wikimedia websites, private and semi-private "wikis" that only certain users can read or edit, questions, comments, or complaints that community members submit to Wikimedia about the performance and operation of its websites, private deliberations of user-community leaders who help administer the Wikimedia websites, emails between registered Wikimedia users, and emails on Wikimedia's mailing lists.

INTERROGATORY NO. 5:

For each category of Wikimedia international, text-based, Internet communications identified in response to Interrogatory No. 3, above, that Plaintiff contends is intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance, please identify the Internet circuits entering or exiting the United States that have carried that category of communication in the past 24 months. To identify a circuit means to state its location of entry to or exit from the United States, to state its country (or, if unknown, global region(s)) of origin or termination abroad, and to identify the person(s) owning or controlling it.

RESPONSE TO INTERROGATORY NO. 5:

In addition to the General Objections above which are incorporated herein, Plaintiff also objects that this Interrogatory is overbroad and unduly burdensome. Plaintiff further objects that this Interrogatory seeks information that is not reasonably calculated to lead to the discovery of admissible evidence. Plaintiff further objects that this Interrogatory seeks information that is within Defendants' control.

Plaintiff also objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff additionally objects that these matters may be the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time.

Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery.

On the basis of these General and Specific Objections, Plaintiff will not provide a response to this Interrogatory.

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 5:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement as discovery in this case continues, Plaintiff supplements its response as follows: As Wikimedia exchanges more than one trillion communications each year with users scattered across the global network, its communications are routed across virtually every major circuit carrying public Internet traffic between the United States and the rest of the world.

INTERROGATORY NO. 6:

For each category of Wikimedia international, text-based, Internet communications identified in response to Interrogatory No. 3, above, that Plaintiff contends is intercepted, copied,

and reviewed by the NSA in the course of Upstream surveillance, please identify each foreign country to or from which such Wikimedia communications were sent in the past 24 months.

RESPONSE TO INTERROGATORY NO. 6:

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory is overbroad, unduly burdensome and seeks information that is not reasonably calculated to lead to the discovery of admissible evidence. Plaintiff also objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff further objects that this Interrogatory seeks information that exceeds the scope of jurisdictional discovery as defined by Defendants, see ECF No. 116 at 4, and as ordered by the Court.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

(1) Wikimedia communications with its community members. Between April 23, 2017 and December 31, 2017, Wikimedia's U.S. servers received HTTPS requests from, and transmitted HTTPS responses to, users in at least 242 non-U.S. countries, territories and regions. This figure is an estimate that was derived using MaxMind geolocation data to determine the country associated with the client IP of each HTTPS request transmitted to Wikimedia's servers in the United States.

(2) Wikimedia's internal log communications. Every time Wikimedia receives an HTTPS request from a person accessing a Wikimedia Project webpage, it creates a corresponding log entry. Between April 23, 2017 and December 31, 2017, Wikimedia's servers in Amsterdam transmitted over 970 billion logs to Wikimedia's servers in the United States.

(3) Electronic communications of Wikimedia staff. Between January 1, 2015 and

December 12, 2017, Wikimedia's office network router located in the United States sent Internet communications to at least approximately 221 non-U.S. countries, territories and regions.

This figure represents Internet outbound communications sent via the following Internet protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

This figure includes communications sent through Wikimedia's Virtual Private Network (VPN).

This figure does not account for the significant number of Internet communications by Wikimedia staff and contractors located internationally, who did not communicate using Wikimedia's Virtual Private Network, but who routinely communicate with Wikimedia staff located at the U.S. headquarters. Between January 1, 2015 and December 22, 2017, Wikimedia engaged over 80 contractors, located across more than 30 different countries.

The results of these analyses will be produced to Defendants. An anonymized list of Plaintiff's contractors located abroad will also be produced to Defendants.

AMENDED RESPONSE TO INTERROGATORY NO. 6:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement or amend its response as discovery in this case continues, Plaintiff amends its response as follows:

(1) Wikimedia communications with its community members. Between April 23, 2017 and December 31, 2017, Wikimedia's U.S. servers received HTTP/S requests from, and transmitted HTTP/S responses to, users in at least 242 non-U.S. countries, territories and regions. This figure is an estimate that was derived using MaxMind geolocation data to determine the country associated with the client IP of each HTTPS request transmitted to Wikimedia's servers

in the United States.

(2) Wikimedia's internal log communications. Every time Wikimedia receives an HTTP/S request from a person accessing a Wikimedia Project webpage, it creates a corresponding log entry. Between April 23, 2017 and December 31, 2017, Wikimedia's servers in Amsterdam transmitted approximately over 970 billion logs to Wikimedia's servers in the United States.

(3) Electronic communications of Wikimedia staff. Between January 1, 2015 and December 12, 2017, Wikimedia's office network router located in the United States logged open Internet connections with at least approximately 221 non-U.S. countries, territories and regions.

This figure represents Internet outbound communications sent via the following Internet protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

This figure includes, but is not limited to, certain communications sent through Wikimedia's Virtual Private Network (VPN).

This figure does not account for a significant number of Internet communications by Wikimedia staff and contractors located internationally who routinely communicate with Wikimedia staff and others located in the United States without using Wikimedia's Virtual Private Network. Between January 1, 2015 and December 22, 2017, Wikimedia engaged over 140 contractors, located across approximately 45 different countries.

The results of these analyses have been produced to Defendants. *See* WIKI0006146, WIKI0006147, WIKI0006148, WIKI0006149, WIKI0006282, WIKI0006368. An anonymized list of Plaintiff's contractors located abroad has also been produced to Defendants. *See* WIKI0006367.

INTERROGATORY NO. 7:

For each category of Wikimedia international, text-based, Internet communications identified in response to Interrogatory No. 3, above, that Plaintiff contends is intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance, please state the total number of such Wikimedia communications made to and from the United States each year for the years 2008-2017, specifying in each case the manner in which Wikimedia counts the communications in that category (e.g., by site visit, page view, HTTP or HTTPS transmissions, e-mails, other forms of messaging, etc.).

RESPONSE TO INTERROGATORY NO. 7:

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory is vastly overbroad, unduly burdensome and seeks information that is not reasonably calculated to lead to the discovery of admissible evidence. Plaintiff also objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff further objects that this Interrogatory seeks information that exceeds the scope of jurisdictional discovery as defined by Defendants, see ECF No. 116 at 4, and as ordered by the Court.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

(1) Wikimedia communications with its community members. Between April 23, 2017 and December 31, 2017, Wikimedia's U.S. servers received over 500 billion HTTPS requests from users outside of the United States. Each HTTPS request generates a corresponding response: thus Wikimedia exchanged over 1 trillion HTTPS requests and responses with its users between April 23, 2017 and December 31, 2017. These figures are estimates that were derived

using MaxMind geolocation data to determine the country associated with the client IP of each HTTPS request transmitted to Wikimedia's servers in the United States.

(2) Wikimedia's internal log communications. Between April 23, 2017 and December 31, 2017, Wikimedia's servers in Amsterdam transmitted approximately over 970 billion logs to Wikimedia's servers in the United States.

(3) Electronic communications of Wikimedia staff. Between June 4, 2014 and December 12, 2017, Wikimedia's office network router located in the United States made at least approximately 22,934,372 Internet connections to 223 non-U.S. countries, territories and regions.

This figure is an estimate and was derived using a geolocation database that catalogues the IP addresses associated with each country, territory and region for each log entry obtained from the Wikimedia Foundation's office router.

This figure represents the total number of Internet outbound connections sent via the following Internet protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

This figure includes connections sent through Wikimedia's Virtual Private Network (VPN).

This figure does not account for the significant number of Internet communications by Wikimedia staff and contractors located internationally who did not communicate using Wikimedia's Virtual Private Network, but who routinely communicate with Wikimedia staff located at the U.S. headquarters. Between January 1, 2015 and December 22, 2017, Wikimedia engaged over 80 contractors, located across more than 30 different countries.

The results of these analyses will be produced to Defendants. An anonymized list of Plaintiff's contractors located abroad will also be produced to Defendants.

AMENDED RESPONSE TO INTERROGATORY NO. 7:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement or amend its response as discovery in this case continues, Plaintiff amends its response as follows:

(1) Wikimedia communications with its community members. Between April 23, 2017 and December 31, 2017, Wikimedia's U.S. servers received approximately over 511 billion HTTP/S requests from users outside of the United States. Each HTTP/S request generates a corresponding response; thus Wikimedia exchanged over 1 trillion HTTP/S requests and responses with its users between April 23, 2017 and December 31, 2017.

These figures are estimates that were derived using MaxMind geolocation data to determine the country associated with the client IP of each HTTP/S request transmitted to Wikimedia's servers in the United States.

(2) Wikimedia's internal log communications. Between April 23, 2017 and December 31, 2017, Wikimedia's servers in Amsterdam transmitted approximately over 970 billion logs to Wikimedia's servers in the United States.

(3) Electronic communications of Wikimedia staff. Between June 4, 2014 and December 12, 2017, Wikimedia's office network router located in the United States logged open Internet connections at least approximately 22,934,372 times, with 223 non-U.S. countries, territories and regions.

This figure is an estimate and was derived using a geolocation database that catalogues the IP addresses associated with each country, territory and region for each log entry obtained from the Wikimedia Foundation's office router.

This figure represents the total number of Internet outbound connections sent via the

following Internet protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

This figure includes, but is not limited to, connections sent through Wikimedia's Virtual Private Network (VPN).

This figure does not account for a significant number of Internet communications by Wikimedia staff and contractors located internationally who routinely communicate with Wikimedia staff and others located in the United States without using Wikimedia's Virtual Private Network. Between January 1, 2015 and December 22, 2017, Wikimedia engaged over 140 contractors, located across approximately 45 different countries.

The results of these analyses have been produced to Defendants. *See* WIKI0006146, WIKI0006147, WIKI0006148, WIKI0006149, WIKI0006282, WIKI0006368. An anonymized list of Plaintiff's contractors located abroad has also been produced to Defendants. *See* WIKI0006367.

INTERROGATORY NO. 8:

For each category of Wikimedia international, text-based, Internet communications identified in response to Interrogatory No. 3, above, that Plaintiff contends is intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance, please state by foreign country the number of such Wikimedia communications made to or from the United States each year for the years 2008-2017, specifying in each case the manner in which Wikimedia counts the communications in that category (e.g., by site visit, page view, HTTP or HTTPS transmissions, e-mails, other forms of messaging, etc.).

RESPONSE TO INTERROGATORY NO. 8:

In addition to the General Objections above which are incorporated herein, Plaintiff

further objects that this Interrogatory is vastly overbroad, unduly burdensome and seeks information that is not reasonably calculated to lead to the discovery of admissible evidence. Plaintiff also objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff further objects that this Interrogatory seeks information that exceeds the scope of jurisdictional discovery as defined by Defendants, *see* ECF No. 116 at 4, and as ordered by the Court. Plaintiff additionally objects to this Interrogatory as duplicative of other written discovery propounded by Defendants.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

(1) Wikimedia communications with its community members. The number of HTTPS requests that Wikimedia's U.S. servers received from users in each country, territory, or region between April 23, 2017 and December 31, 2017 is attached as Exhibit B and will be included in a forthcoming production to Defendants. Each HTTPS request generates a corresponding response that is not reflected in the figures included in this analysis. These figures are estimates that were derived using MaxMind geolocation data to determine the country associated with the client IP of each HTTPS request transmitted to Wikimedia's servers in the United States.

(2) Wikimedia's internal log communications. Between April 23, 2017 and December 31, 2017, Wikimedia's servers in Amsterdam transmitted over 970 billion logs to Wikimedia's servers in the United States.

(3) Electronic communications of Wikimedia staff. Between June 4, 2014 and December 12, 2017, Wikimedia's office network router located in the United States sent at least approximately 22,934,372 Internet connections to at least 223 non-U.S. countries, territories and

regions. A list of the numbers of these communications broken down by country, territory, or region will be produced to Defendants.

These figures are estimates and were derived using a geolocation database that catalogues the IP addresses associated with each country, territory and region for each log entry obtained from the Wikimedia Foundation's office router.

These figures represent the total number of Internet outbound connections sent via the following Internet protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

These figures include connections sent through Wikimedia's Virtual Private Network (VPN).

These figures do not account for the significant number of Internet communications by Wikimedia staff and contractors located internationally who did not communicate using Wikimedia's Virtual Private Network, but who routinely communicate with Wikimedia staff located at the U.S. headquarters. Between January 1, 2015 and December 22, 2017, Wikimedia engaged over 80 contractors, located across more than 30 different countries.

The results of these analyses will be produced to Defendants. An anonymized list of Plaintiff's staff and contractors located abroad will also be produced to Defendants.

AMENDED RESPONSE TO INTERROGATORY NO. 8:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement or amend its response as discovery in this case continues, Plaintiff amends its response as follows:

(1) Wikimedia communications with its community members. The number of HTTP/S requests that Wikimedia's U.S. servers received from users in each country, territory, or

region between April 23, 2017 and December 31, 2017 is attached as Amended Exhibit B. Each HTTP/S request generates a corresponding response that is not reflected in the figures included in this analysis. These figures are estimates that were derived using MaxMind geolocation data to determine the country associated with the client IP of each HTTP/S request transmitted to Wikimedia's servers in the United States.

(2) Wikimedia's internal log communications. Between April 23, 2017 and December 31, 2017, Wikimedia's servers in Amsterdam transmitted approximately over 970 billion logs to Wikimedia's servers in the United States.

(3) Electronic communications of Wikimedia staff. Between June 4, 2014 and December 12, 2017, Wikimedia's office network router located in the United States logged open Internet connections at least approximately 22,934,372 times with 223 non-U.S. countries, territories and regions. A list of the numbers of these communications broken down by country, territory, or region will be produced to Defendants.

This figure is an estimate and was derived using a geolocation database that catalogues the IP addresses associated with each country, territory and region for each log entry obtained from the Wikimedia Foundation's office router.

This figure represents the total number of Internet outbound connections sent via the following Internet protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

This figure includes, but is not limited to, connections sent through Wikimedia's Virtual Private Network (VPN).

This figure does not account for a significant number of Internet communications by Wikimedia staff and contractors located internationally who routinely communicate with

Wikimedia staff and others located in the United States without using Wikimedia's Virtual Private Network. Between January 1, 2015 and December 22, 2017, Wikimedia engaged over 140 contractors, located across approximately 45 different countries.

The results of these analyses have been produced to Defendants. *See* WIKI0006146, WIKI0006147, WIKI0006148, WIKI0006149, WIKI0006282, WIKI0006368. An anonymized list of Plaintiff's staff and contractors located abroad has also been produced to Defendants. *See* WIKI0006367.

INTERROGATORY NO. 11:

Please state the basis of Plaintiff's allegations, in paragraphs 61, 85, and 88 of the Amended Complaint, that Wikimedia's alleged "community of volunteers, contributors, and readers consists of individuals in virtually every country on earth" and that Wikimedia "communicate[s] with individuals in virtually every country on earth."

RESPONSE TO INTERROGATORY NO. 11:

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is overbroad and duplicative of other written discovery propounded by Defendants. Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

Numerous facts support Wikimedia's allegations that its "community of volunteers, contributors, and readers consists of individuals in virtually every country on earth" and that Wikimedia engages in "communications . . . with individuals in virtually every country on earth." As explained in Wikimedia's responses to NSA Interrogatory Nos. 6-8, Wikimedia users from all over the world read and contribute to Wikimedia's Project pages. This analysis is further supported by statistics showing that Wikimedia's Project pages are viewed by millions of

users around the world. Wikimedia publishes current monthly page view statistics by country (*available* at https://stats.wikimedia.org/wikimedia/squids/SquidReportPageViewsPerCountryOverview.htm), and maintains an archive with analogous data for past months (*available* at https://stats.wikimedia.org/archive/squid_reports/).

Wikimedia also has dozens of foreign independent but associated entities, including user groups, chapters and thematic organizations. *See* https://meta.wikimedia.org/wiki/Wikimedia_movement_affiliates#chapters.

In the last two years alone, Wikimedia has awarded grants and scholarships to users and programs in dozens of countries. Additionally, Wikimedia projects are currently active in 288 languages, further underscoring Wikimedia's global presence. *See* https://en.wikipedia.org/wiki/List_of_Wikipedias.

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 11:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement its response as discovery in this case continues, Plaintiff supplements its response as follows:

Wikimedia also maintains a publicly available repository of data that allows for various analyses of Wikimedia project page views by country (*available* at https://wikitech.wikimedia.org/wiki/Analytics/AQS/Pageviews).

Numerous documents in Plaintiff's production support its allegations that its "community of volunteers, contributors, and readers consists of individuals in virtually every country on earth" and that Wikimedia engages in "communications . . . with individuals in virtually every country on earth," including, *inter alia*, Amended Exhibit B: WIKI0006367 (listing international

Wikimedia contractors); WIKI0002407 (listing 288 Wikipedia language editions); WIKI0002416 (listing Wikimedia movement affiliates); WIKI0006369 (listing page views for virtually every country on earth); WIKI0002360, WIKI0002365, WIKI0002367, WIKI0002389, WIKI0002396 (noting countries involved in user grants and scholarships); WIKI0006295 (listing funded grants by country).

ALLEGATIONS REGARDING NSA INTERCEPTION OF WIKIMEDIA'S INTERNATIONAL, TEXT-BASED, INTERNET COMMUNICATIONS

INTERROGATORY NO. 13:

Please identify each of the international Internet "backbone chokepoints," whether cables, circuits, or other communications facilities, at which Plaintiff contends, in paragraph 66 of the Amended Complaint, the NSA must be conducting Upstream surveillance, stating for each such "backbone chokepoint" the basis of Plaintiff's contention.

RESPONSE TO INTERROGATORY NO. 13:

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff also objects that this Interrogatory seeks information that is within Defendants' control. Plaintiff further objects that this Interrogatory is a contention Interrogatory that is premature at this stage in the litigation. Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

An NSA document states that the NSA has established interception capabilities on "many of the chokepoints operated by U.S. providers through which international communications enter and leave the United States." *See* NSA Staff Processing Form, Subject: SSO's Support to the

FBI for Implementation of their Cyber FISA Orders.

The "chokepoints" at which the NSA conducts Upstream surveillance have included the "seven access sites" identified in an NSA document, reproduced at paragraph 68 of Plaintiff's First Amended Complaint (ECF No. 70-1).

Additional reporting after the filing of the Amended Complaint states that the NSA has installed surveillance equipment in at least 17 "internet hubs" operated by another major U.S. telecommunications provider. *See* Julia Angwin et al., *NSA Spying Relies on AT&T's 'Extreme Willingness to Help'*, ProPublica, Aug. 15, 2015 (and associated documents, one of which describes the surveillance of hundreds of circuits at a specific AT&T trans-Pacific cable site); Julia Angwin & Jeff Larson, *New Snowden Documents Reveal Secret Memos Expanding Spying*, ProPublica, June 4, 2015 (and associated documents); Jeff Larson et al., *A Trail of Evidence Leading to AT&T's Partnership with the NSA*, ProPublica, Aug. 15, 2015 (and associated documents) (describing surveillance on AT&T's network, including on "OC-192 and 10GE peering circuits"; describing surveillance on Verizon's network, including at a cable-landing site called BRECKENRIDGE).

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 13:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement as discovery in this case continues, Plaintiff supplements its response as follows:

The bases for Plaintiff's contention also include the following: Glenn Greenwald, *No Place to Hide* (2014).

INTERROGATORY NO. 15:

Please state the basis of Plaintiff's contentions regarding the manner in which the alleged

copying, filtering, and content-review processes referred to in paragraph 49 of the Amended Complaint are carried out.

RESPONSE TO INTERROGATORY NO. 15:

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is a contention Interrogatory that is premature at this stage in the litigation. Plaintiff additionally objects that these matters may be the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time.

Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery. Plaintiff also objects that this Interrogatory is overbroad and duplicative of other written discovery propounded by Defendants.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

The bases of Plaintiff's contentions are the principles of Internet communication and the technical necessities of the inspection of Internet communications in transit.

For example, Internet communications in transit are split into packets. Where an eavesdropper is attempting to determine whether the contents of a particular communication in transit on the Internet contain a particular piece of information, the eavesdropper generally must reassemble the packets constituting the communication and then scan the reassembled communication. Reassembling Internet packets requires the temporary copying (or "caching") of those packets until all packets needed for the reassembly have arrived.

Additionally, Upstream surveillance involves the retention of communications that contain targeted selectors. To retain a communication in transit, an eavesdropper must copy and reassemble the packets constituting the communication. But because an eavesdropper cannot

know in advance which packets in transit are part of a communication containing a targeted selector, the eavesdropper must create a temporary copy of all packets that might be a part of such a communication.

In addition, a *New York Times* report from August 2013 states, based on a review of NSA documents and interviews with senior intelligence officials, that "the N.S.A. is temporarily copying and then sifting through the contents of what is apparently most e-mails and other text-based communications that cross the border." Charlie Savage, *N.S.A Said to Search Content of Messages to and from U.S.*, N.Y. Times, Aug. 8, 2013; *see also* Charlie Savage, *Power Wars* 207–11 (2015).

Other bases of Plaintiff's contentions include:

- The PCLOB Report, including pages 7–10, 12–13, 22, 30–41 & n.157, 79, 111 n.476, 120–22, 125, 143, and official government sources concerning Upstream surveillance cited therein.
- [*Redacted*], No. [Redacted], 2011 WL 10945618 (FISC Oct. 3, 2011)
- 50 U.S.C. §§ 1801, 1881a.
- David S. Kris & J. Douglas Wilson, *National Security Investigations and Prosecutions* § 17.5 (July 2015)
- Julia Angwin et al., *NSA Spying Relies on AT&T's 'Extreme Willingness to Help'*, ProPublica, Aug. 15, 2015 (and associated documents)
- Julia Angwin & Jeff Larson, *New Snowden Documents Reveal Secret Memos Expanding Spying*, ProPublica, June 4, 2015 (and associated documents)
- Jeff Larson et al., *A Trail of Evidence Leading to AT&T's Partnership with the NSA*, ProPublica, Aug. 15, 2015 (and associated documents)

- PCLOB, Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 26:15–18 (Mar. 19, 2014) (statement of Robert Litt, General Counsel, ODNI)
- Charlie Savage, *Power Wars* (2015)

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 15:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement as discovery in this case continues, Plaintiff supplements its response as follows:

The bases for Plaintiff's contention also include the following: Glenn Greenwald, *No Place to Hide* (2014).

INTERROGATORY NO. 21:

To the extent not already stated or identified in response to Interrogatory Nos. 13-20, above, or in response to Defendant United States Department of Justice's First Set of Interrogatories, Interrogatory Nos. 1-6, please state the basis of Plaintiff's contention that the NSA is intercepting, copying, and reviewing at least some of its communications.

RESPONSE TO INTERROGATORY NO. 21:

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is a contention Interrogatory that is premature at this stage in the litigation. Plaintiff also objects that this Interrogatory seeks information that is the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time. Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery. Plaintiff also objects that this Interrogatory is overbroad and duplicative of other written discovery propounded by Defendants.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

Plaintiff's contention is based on the volume and distribution of its communications, basic principles governing the routing and transmission of Internet communications, and basic principles governing how surveillance on a packet-switched network operates.

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 21:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement as discovery in this case continues, Plaintiff supplements its response as follows:

The bases for Plaintiff's contention also include the following:

- Exhibits A–F to Plaintiff's First Set of Requests for Admission
- WIKI0008024 (slide deck from which Exhibit B to Plaintiff's First Set of Requests for Admission was excerpted, entitled "XKEYSCORE for Counter-CNE")
- Glenn Greenwald, *Xkeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet'*, The Guardian, July 31, 2013 (and associated documents).
- Barton Gellman, Julie Tate, & Ashkan Soltani, *In NSA-intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are*, Wash. Post, July 5, 2014.

Dated: March 23, 2018

/s/Ashley Gorski
Ashley Gorski
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
agorski@aclu.org

Counsel for Plaintiff Wikimedia Foundation, Inc.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, Plaintiff, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	Civil Action No. 1:15-cv-00662-TSE

Attachment F

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, Plaintiff, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	Civil Action No. 1:15-cv-00662-TSE ~~FILED UNDER SEAL~~

EXHIBIT 4

IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, INC. Plaintiff, v. NATIONAL SECURITY AGENCY, et al., Defendants.	Civil Action No. 1:15-cv-00662-TSE Hon. T.S. Ellis, III

WIKIMEDIA FOUNDATION, INC.'S AMENDED RESPONSES AND OBJECTIONS TO OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE'S INTERROGATORY NO. 19

PROPOUNDING PARTY: **OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE**

RESPONDING PARTY: **WIKIMEDIA FOUNDATION, INC.**

SET NUMBER: **THREE**

Pursuant to Federal Rule of Civil Procedure 33, Plaintiff Wikimedia Foundation, Inc. ("Plaintiff" or "Wikimedia") responds as follows to Defendant Office of the Director of National Intelligence's ("Defendant" or "ODNI") (collectively with Plaintiff, the "Parties") Interrogatory No. 19 (the "Interrogatory"):

I. GENERAL RESPONSES.

1. Plaintiff's response to Defendant's Interrogatory is made to the best of Plaintiff's present knowledge, information, and belief. Discovery in this action is ongoing, and Plaintiff's responses may be substantially altered by further investigation, including further review of Plaintiff's own documents, as well as the review of documents produced by Defendant. Said response is at all times subject to such additional or different information that discovery or further investigation may disclose and, while based on the present state of Plaintiff's recollection, is

subject to such refreshing of recollection, and such additional knowledge of facts, as may result from Plaintiff's further discovery or investigation.

2. Plaintiff reserves the right to make any use of, or to introduce at any hearing and at trial, information and/or documents responsive to Defendant's Interrogatory but discovered subsequent to the date of this response, including, but not limited to, any such information or documents obtained in discovery herein.

3. To the extent that Plaintiff responds to Defendant's Interrogatory by stating that Plaintiff will provide information and/or documents that Plaintiff deems to embody material that is private, business confidential, proprietary, trade secret, or otherwise protected from disclosure pursuant to Federal Rule of Civil Procedure 26(c)(7), Federal Rule of Evidence 501, or other applicable law, Plaintiff will do so only pursuant to the Parties' Stipulated Protective Order (ECF No. 120).

4. Plaintiff reserves all objections or other questions as to the competency, relevance, materiality, privilege, or admissibility as evidence in any subsequent proceeding in or trial of this or any other action for any purpose whatsoever of Plaintiff's responses herein and any document or thing identified or provided in response to Defendant's Interrogatory.

5. Plaintiff's responses will be subject to and limited by any agreements the Parties reach concerning the scope of discovery.

6. Plaintiff reserves the right to object on any ground at any time to such other or supplemental interrogatories as Defendant may at any time propound involving or relating to the subject matter of this Interrogatory.

II. GENERAL OBJECTIONS.

Plaintiff makes the following general objections, whether or not separately set forth in

response to the Interrogatory, to each instruction, definition, and Interrogatory made in Defendant ODNI's Interrogatories, Set Three:

1. Plaintiff objects to the Interrogatory in its entirety insofar as the instructions, definitions, or Interrogatory seeks information or production of documents protected by the attorney-client privilege or the work product doctrine. Fed. R. Civ. Proc. 26(b)(1). Such information or documents shall not be provided in response to Defendant's Interrogatory and any inadvertent disclosure or production thereof shall not be deemed a waiver of any privilege with respect to such information or documents or of any work product immunity which may attach thereto. Fed. R. Civ. Proc. 26(b)(5)(B).

2. Plaintiff objects to the Interrogatory in its entirety to the extent the instruction, definition, or Interrogatory seeks identification of documents, witnesses, or information that Defendant has withheld from Plaintiff. Fed. R. Civ. Proc. 26(b)(1), (2).

3. Plaintiff objects to the Interrogatory in its entirety to the extent it requires Plaintiff to identify potentially thousands of pages of documents, not all of which have been or can be located and reviewed by counsel within the time period allowed for this response or within a reasonable time. Accordingly, the Interrogatory would subject Plaintiff to unreasonable and undue annoyance, oppression, burden and expense.

4. Plaintiff objects to the extent the Interrogatory exceeds the scope of jurisdictional discovery as defined by Defendants, *see* ECF No. 116 at 4, and ordered by the Court. *See* ECF No. 117.

5. Plaintiff objects to the Interrogatory in its entirety to the extent it seeks information that is available through or from public sources or records, or that is otherwise equally available to Defendant, on the ground that it unreasonably subjects Plaintiff to undue annoyance, oppression,

burden, and expense. Fed. R. Civ. Proc. 26(b)(1), (2).

6. Plaintiff objects to the Interrogatory in its entirety to the extent it purports to impose obligations that are greater or more burdensome than or contradict those imposed by the applicable Federal and local rules. *See* Fed. R. Civ. Proc. 26, 33.

7. Plaintiff objects to the Interrogatory in its entirety as Defendant's Interrogatories in aggregate contain more than the "25 written interrogatories, including all discrete subparts," permitted by the Federal Rules of Civil Procedure, Rule 33(a)(1), and Defendant has not sought leave to serve additional interrogatories.

8. Plaintiff objects to the Interrogatory in its entirety to the extent it seeks documents or information no longer in existence or not currently in Plaintiff's possession, custody, or control, or to the extent it refers to persons, entities, or events not known to Plaintiff or controlled by Plaintiff, on the grounds that such definitions or Interrogatories are overly broad, seek to require more of Plaintiff than any obligation imposed by law, would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense, and would seek to impose upon Plaintiff an obligation to investigate, discover, or produce information or materials from third parties or otherwise that are accessible to Defendant or readily obtainable from public or other sources. Fed. R. Civ. Proc. 26(b)(1), (2).

9. Plaintiff objects to the Interrogatory in its entirety to the extent it seeks information or production of documents protected from disclosure by any right to privacy or any other applicable privilege or protection, including the right to confidentiality or privacy of third parties, any right of confidentiality provided for by Plaintiff's contracts or agreements with such third parties, or by Plaintiff's obligations under applicable law or contract to protect such confidential information. Plaintiff reserves the right to withhold any responsive information or documents

governed by a third-party confidentiality agreement until such time as the appropriate notice can be given or the appropriate permissions can be obtained. Plaintiff also objects generally to all instructions, definitions, or the Interrogatory to the extent it seeks disclosure of trade secrets and other confidential research or analyses, development, or commercial information of Plaintiff or any third party.

10. Plaintiff objects to the Interrogatory in its entirety to the extent it is overbroad and unduly burdensome, particularly to the extent they seek "all," "each," or "any" documents, witnesses, individuals, persons, organizations, statements, or facts that refer or relate to various subject matters. Fed. R. Civ. Proc. 26(b)(1), (2). To the extent Plaintiff responds to the Interrogatory, Plaintiff will use reasonable diligence to identify responsive documents, witnesses, individuals, persons, organizations, statements, or facts in its possession, custody, or control, based on its present knowledge, information, and belief.

11. Plaintiff objects to the Interrogatory in its entirety to the extent it seeks expert discovery prematurely.

12. Plaintiff objects to the Interrogatory in its entirety to the extent it purports to require Plaintiff to restore and/or search data sources that are not reasonably accessible on the grounds that such definitions and Interrogatory would subject Plaintiff to undue burden and expense. Fed. R. Civ. Proc. 26(b)(1), (2).

III. DEFINITIONAL OBJECTIONS.

1. Plaintiff objects to definition number one (1) to the extent it defines "Plaintiff" and "Wikimedia" to include Plaintiff's "parent, subsidiary, and affiliated organizations, and all persons acting on their behalf, including officials, agents, employees, attorneys, and consultants." Said definition is overly broad, seeks irrelevant information not calculated to lead to the discovery of

admissible evidence, seeks information outside Plaintiff's possession, custody, or control, and would subject Plaintiff to unreasonable and undue annoyance, oppression, burden and expense. Said definition is also vague and ambiguous in that it cannot be determined what is meant by the terms "affiliated organizations" and "all persons acting on their behalf." Plaintiff shall construe "Plaintiff" and "Wikimedia" to mean Wikimedia, and its present officers, directors, agents, and employees.

2. Plaintiff objects to the definition of "identify" with respect to Internet Protocol ("IP") addresses because this definition calls for a significant and burdensome collection of information in addition to the IP addresses themselves. The additional information called for by the definition of "identify" is overbroad, unduly burdensome, not proportional and seeks information that is not reasonably calculated to lead to the discovery of admissible evidence relevant to jurisdictional issues.

IV. INSTRUCTIONAL OBJECTIONS

1. Plaintiff objects to instruction number one (1) to the extent it purports to request "knowledge or information" from Wikimedia's "parent, subsidiary, or affiliated organizations, and their officials, agents, employees, attorneys, consultants, and any other person acting on their behalf." Said request is overly broad, seeks irrelevant information not calculated to lead to the discovery of admissible evidence, seeks information outside Plaintiff's possession, custody, or control, and would subject Plaintiff to unreasonable and undue annoyance, oppression, burden and expense. Moreover, said request is vague and ambiguous in that it cannot be determined what is meant by the term "affiliated organizations" and "any other person acting on their behalf." Where an Interrogatory requests knowledge or information of Plaintiff, Plaintiff shall construe such request to mean knowledge or information from Wikimedia, and its present officers, directors,

agents, and employees.

2. Plaintiff objects to instruction number two (2) as unduly burdensome to the extent it imposes an obligation to provide information greater than that required by the Federal Rules of Civil Procedure.

3. Plaintiff objects to instruction number three (3) as unduly burdensome and imposing an obligation to provide information greater than that required by the Federal Rules of Civil Procedure to the extent it purports to require Plaintiff to "identify each person known by Plaintiff to have such knowledge, and in each instance where Plaintiff avers insufficient knowledge or information as a grounds for not providing information or for providing only a portion of the information requested, set forth a description of the efforts made to locate information needed to answer the interrogatory."

4. Plaintiff objects to instruction number four (4) to the extent it seeks to require it to identify anything other than the specific claim of privilege or work product being made and the basis for such claim, and to the extent it seeks to require any information not specified in Discovery Guideline 10, on the grounds that the additional information sought by Defendant would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense, and constitutes information protected from discovery by privilege and as work product. Plaintiff is willing to discuss acceptable reciprocal obligations for disclosure of information withheld on the basis of attorney-client privilege or attorney work-product.

5. Plaintiff objects to instruction number five (5) that the Interrogatory is continuing, to the extent said instruction seeks unilaterally to impose an obligation to provide supplemental information greater than that required by Federal Rule of Civil Procedure 26(e) and would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense. Plaintiff will

comply with the requirements of the Federal Rules of Civil Procedure and is willing to discuss mutually acceptable reciprocal obligations for continuing discovery.

V. SPECIFIC OBJECTIONS AND RESPONSE TO INTERROGATORY NO. 19.

Without waiving or limiting in any manner any of the foregoing General Objections, Definitional Objections, or Instructional Objections, but rather incorporating them into the following response to the extent applicable, Plaintiff responds to Defendant's Interrogatory No. 19 as follows:

INTERROGATORY NO. 19:

NSA Interrogatory No. 3 requests that Plaintiff identify each category of Wikimedia international, text-based, Internet communications that Plaintiff contends is intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance. For the period January 1, 2017, to the present, please describe the communications in each such category by stating:

> a. each communications protocol used to transmit Wikimedia communications in that category;
>
> b. the number, to the extent it is known or can be estimated, of Wikimedia communications in that category using each protocol;
>
> c. to the extent known, the countries to and from which Wikimedia communications in that category, using each protocol, are transmitted;
>
> d. whether and by what means communications in that category using each type of protocol are encrypted; and
>
> e. the Internet Protocol (IP) addresses or address blocks used by Wikimedia for purposes of transmitting or receiving communications in that category.

If Plaintiff does not intend at summary judgment or trial to offer proof that communications in a given category that use a given protocol are intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance, then it need not identify, quantify, or otherwise respond to this interrogatory concerning communications in that category using that protocol.

RESPONSE TO INTERROGATORY NO. 19:

In addition to Plaintiff's General Objections, which are incorporated herein, Plaintiff objects to this Interrogatory because it is improperly compound and contains multiple subparts. Plaintiff also objects that this Interrogatory is vague and ambiguous as to its use of the term "communications protocol." Plaintiff further objects that this Interrogatory is overly broad, unduly burdensome, not proportional and seeks information that is not reasonably calculated to lead to the discovery of admissible evidence relevant to jurisdictional issues. Wikimedia objects to the Interrogatory as unreasonably cumulative and duplicative of Defendants' written discovery requests and Wikimedia's written discovery responses and document productions in this matter, including, *inter alia*, NSA Interrogatory Nos. 6-8 and ODNI Interrogatory Nos. 14-15.

Plaintiff additionally objects to this Interrogatory to the extent that it seeks information that is not within Plaintiff's possession, custody and control or public information that is equally accessible to Defendant. Plaintiff further objects that this Interrogatory seeks information that exceeds the scope of jurisdictional discovery as defined by Defendants, *see* ECF No. 116 at 4, and as ordered by the Court. *See* ECF No. 117. For example, to the extent the Interrogatory seeks information concerning the volume or proportion of Wikimedia communications that are encrypted and the encryption protocols used, Wikimedia objects that such subjects exceed the scope of jurisdictional discovery as defined by Defendants, *see* ECF No. 116 at 4, and as ordered by the Court. *See* ECF No. 117.

On the basis of these General and Specific Objections, Plaintiff will not provide a response to this Interrogatory.

AMENDED RESPONSE TO INTERROGATORY NO. 19:

In addition to Plaintiff's General Objections, which are incorporated herein, Plaintiff objects to this Interrogatory because it is improperly compound and contains multiple subparts. Plaintiff also objects that this Interrogatory is vague and ambiguous as to its use of the term "communications protocol." Plaintiff further objects that this Interrogatory is overly broad, unduly burdensome, not proportional and seeks information that is not reasonably calculated to lead to the discovery of admissible evidence relevant to jurisdictional issues. Wikimedia objects to the Interrogatory as unreasonably cumulative and duplicative of Defendants' written discovery requests and Wikimedia's written discovery responses and document productions in this matter, including, *inter alia*, NSA Interrogatory Nos. 6-8 and ODNI Interrogatory Nos. 14-15.

Plaintiff additionally objects to this Interrogatory to the extent that it seeks information that is not within Plaintiff's possession, custody and control or public information that is equally accessible to Defendant. Plaintiff further objects that this Interrogatory seeks information that exceeds the scope of jurisdictional discovery as defined by Defendants, *see* ECF No. 116 at 4, and as ordered by the Court. *See* ECF No. 117. For example, to the extent the Interrogatory seeks information concerning the volume or proportion of Wikimedia communications that are encrypted and the encryption protocols used, Wikimedia objects that such subjects exceed the scope of jurisdictional discovery as defined by Defendants, *see* ECF No. 116 at 4, and as ordered by the Court. *See* ECF No. 117.

Subject to and without waiving any of these General or Specific Objections, Plaintiff's response to this Interrogatory is contained in the attached Exhibit 1, and Exhibits A–G.

Dated: April 6, 2018

/s/ Ashley Gorski

Ashley Gorski
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
agorski@aclu.org

Counsel for Plaintiff

EXHIBIT 1

TECHNICAL STATISTICS FOR 2017 TO 2018 RESPONSIVE TO ODNI INTERROGATORY NO. 19						
Protocol	**Volume**	**Date Range**	**Foreign Countries, Regions, Territories**	**IP Addresses**	**Encryption Status**	**Additional Notes**
ODNI Interrogatory 19(a)	*ODNI Interrogatory 19(b)*		*ODNI Interrogatory 19(c)*	*ODNI Interrogatory 19(e)*	*ODNI Interrogatory 19(d)*	*ODNI Interrogatory 19 (d)*
Category 1 Wikimedia communications with its community members, who read and contribute to Wikimedia's Projects and webpages, and who use the Projects and webpages to interact with each other						
Total HTTP & HTTPS requests: foreign users to WMF US servers	381,655,849,279	Aug. 1, 2017, to Jan. 31, 2018 (six months)	List of countries for HTTPS (Exhibit A)	198.35.26.0/23, 208.80.152.0/22, 2620:0:860::/48, 2620:0:861::/48, 2620:0:863::/48	HTTPS: 373,045,851,598	For clarity, these HTTPS and HTTP requests use the same IP addresses.
			List of countries for HTTP (Exhibit B)		HTTP: 8,609,997,681	
Total HTTP & HTTPS requests: US users to WMF foreign servers	2,812,819,460	Aug. 1, 2017, to Jan. 31, 2018 (six months)	Netherlands	91.198.174.0/24, 2620:0:862::/48	HTTPS: 2,479,014,613	For clarity, these HTTPS and HTTP requests use the same IP addresses.
					HTTP: 333,804,847	
SMTP communications: foreign users to WMF US servers	Unknown		Unknown	208.80.152.0/22, 2620:0:860::/48, 2620:0:861::/48	Unknown	
Category 2 Wikimedia's internal log communications						
Apache Kafka log communications transmitted from WMF foreign servers to WMF US servers	736,045,377,450	Aug. 1, 2017, to Jan. 31, 2018 (six months)	Netherlands	10.0 0 0/8, 2620:0:860: /46	736,045,377,450 log communications encrypted using IPSec	
Category 3 Communications by Wikimedia staff						
Logged international TCP connections using WMF Office Network or WMF VPN	4,948,011	Mar. 1, 2017 to Feb. 28, 2018 (one year)	List of countries for non-VPN (Exhibit C); List of countries for VPN (Exhibit D)	The WMF Office Network IP range is 198.73.209 0/24, with the WMF VPN operating on IP address 198.73.209 25	All 791 connections encrypted using OpenVPN (SSL/TLS protocol)	Other than the VPN connections, Wikimedia itself does not systematically encrypt connections to and from the office network router and it would not be practical for it to do so. However, individuals who use the office network router may establish encrypted connections based on the particular communications services they use at any given time. Because Wikimedia's office network router does not log application-layer protocol information, Wikimedia does not know with certainty the extent to which the data transmitted over these non-VPN connections is encrypted. The logs do contain, however, the source and destination ports of connections, which in certain cases may shed light on the encryption status of connections, such as those that use port 443 or port 22.

[redacted]

[redacted]

Logged international UDP connections using WMF Office Network or WMF VPN	2,207,771	Mar. 1, 2017 to Feb. 28, 2018 (one year)	List of countries for non-VPN (Exhibit E); List of countries for VPN (Exhibit F)	The WMF Office Network IP range is 198.73.209 0/24, with the WMF VPN operating on IP address 198.73.209 25	All 19,709 connections encrypted using OpenVPN (SSL/TLS protocol)	Same response.
Logged international ICMP connections using WMF Office Network or WMF VPN	51,301	Mar. 1, 2017 to Feb. 28, 2018 (one year)	List of countries for non-VPN (Exhibit G)	The WMF Office Network IP range is 198.73.209 0/24, with the WMF VPN operating on IP address 198.73.209 25	0 connections encrypted using VPN	Same response.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, Plaintiff, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	Civil Action No. 1:15-cv-00662-TSE

Attachment G

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, Plaintiff, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	Civil Action No. 1:15-cv-00662-TSE ~~FILED UNDER SEAL~~

EXHIBIT 5

IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, INC. Plaintiff, v. NATIONAL SECURITY AGENCY, et al., Defendants.	Civil Action No. 1:15-cv-00662-TSE Hon. T.S. Ellis, III

WIKIMEDIA FOUNDATION, INC.'S RESPONSES AND OBJECTIONS TO NATIONAL SECURITY AGENCY'S FIRST SET OF INTERROGATORIES

PROPOUNDING PARTY: **NATIONAL SECURITY AGENCY**

RESPONDING PARTY: **WIKIMEDIA FOUNDATION, INC.**

SET NUMBER: **ONE**

Pursuant to Federal Rule of Civil Procedure 33, Plaintiff Wikimedia Foundation, Inc. ("Plaintiff" or "Wikimedia") responds as follows to Defendant National Security Agency's ("Defendant" or "NSA") (collectively with Plaintiff, the "Parties") First Set of Interrogatories (the "Interrogatories"):

I. GENERAL RESPONSES.

1. Plaintiff's response to Defendant's Interrogatories is made to the best of Plaintiff's present knowledge, information, and belief. Discovery in this action is ongoing, and Plaintiff's responses may be substantially altered by further investigation, including further review of Plaintiff's own documents, as well as the review of documents produced by Defendant, which Plaintiff has just begun to receive. Said response is at all times subject to such additional or different information that discovery or further investigation may disclose and, while based on the

present state of Plaintiff's recollection, is subject to such refreshing of recollection, and such additional knowledge of facts, as may result from Plaintiff's further discovery or investigation.

2. Plaintiff reserves the right to make any use of, or to introduce at any hearing and at trial, information and/or documents responsive to Defendant's Interrogatories but discovered subsequent to the date of this response, including, but not limited to, any such information or documents obtained in discovery herein.

3. To the extent that Plaintiff responds to Defendant's Interrogatories by stating that Plaintiff will provide information and/or documents that Plaintiff deems to embody material that is private, business confidential, proprietary, trade secret, or otherwise protected from disclosure pursuant to Federal Rule of Civil Procedure 26(c)(7), Federal Rule of Evidence 501, or other applicable law, Plaintiff will do so only pursuant to the Parties' Stipulated Protective Order (ECF No. 120).

4. Plaintiff reserves all objections or other questions as to the competency, relevance, materiality, privilege, or admissibility as evidence in any subsequent proceeding in or trial of this or any other action for any purpose whatsoever of Plaintiff's responses herein and any document or thing identified or provided in response to Defendant's Interrogatories.

5. Plaintiff's responses will be subject to and limited by any agreements the Parties reach concerning the scope of discovery.

6. Plaintiff reserves the right to object on any ground at any time to such other or supplemental interrogatories as Defendant may at any time propound involving or relating to the subject matter of these Interrogatories.

II. GENERAL OBJECTIONS.

Plaintiff makes the following general objections, whether or not separately set forth in

response to each Interrogatory, to each instruction, definition, and Interrogatory made in Defendant's Interrogatories:

1. Plaintiff objects to the Interrogatories in their entirety insofar as any such instruction, definition, or Interrogatory seeks information or production of documents protected by the attorney-client privilege or the work product doctrine. Fed. R. Civ. Proc. 26(b)(1). Such information or documents shall not be provided in response to Defendant's Interrogatories and any inadvertent disclosure or production thereof shall not be deemed a waiver of any privilege with respect to such information or documents or of any work product immunity which may attach thereto. Fed. R. Civ. Proc. 26(b)(5)(B).

2. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory seeks identification of documents, witnesses, or information that Defendant has withheld from Plaintiff. Fed. R. Civ. Proc. 26(b)(1), (2).

3. Plaintiff objects to the Interrogatories in their entirety to the extent any such Interrogatory requires Plaintiff to identify potentially thousands of pages of documents, not all of which have been or can be located and reviewed by counsel within the time period allowed for this response or within a reasonable time. Accordingly, said Interrogatories would subject Plaintiff to unreasonable and undue annoyance, oppression, burden and expense.

4. Plaintiff objects to any Interrogatories that exceed the scope of jurisdictional discovery as defined by Defendants, *see* ECF No. 116 at 4, and ordered by the Court.

5. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory seeks information that is available through or from public sources or records, or that are otherwise equally available to Defendant, on the ground that such instructions, definitions, and/or Interrogatories unreasonably subject Plaintiff to undue annoyance,

oppression, burden, and expense. Fed. R. Civ. Proc. 26(b)(1), (2).

6. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory purport to impose obligations that are greater or more burdensome than or contradict those imposed by the applicable Federal and local rules. *See* Fed. R. Civ. Proc. 26, 33.

7. Plaintiff objects to the Interrogatories in their entirety as the Interrogatories contain more than the "25 written interrogatories, including all discrete subparts," permitted by the Federal Rules of Civil Procedure, Rule 33(a)(1), and Defendant has not sought leave to serve additional interrogatories.

8. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory seeks documents or information no longer in existence or not currently in Plaintiff's possession, custody, or control, or to the extent they refer to persons, entities, or events not known to Plaintiff or controlled by Plaintiff, on the grounds that such definitions or Interrogatories are overly broad, seek to require more of Plaintiff than any obligation imposed by law, would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense, and would seek to impose upon Plaintiff an obligation to investigate, discover, or produce information or materials from third parties or otherwise that are accessible to Defendant or readily obtainable from public or other sources. Fed. R. Civ. Proc. 26(b)(1), (2).

9. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory seeks information or production of documents protected from disclosure by any right to privacy or any other applicable privilege or protection, including the right to confidentiality or privacy of third parties, any right of confidentiality provided for by Plaintiff's contracts or agreements with such third parties, or by Plaintiff's obligations under

applicable law or contract to protect such confidential information. Plaintiff reserves the right to withhold any responsive information or documents governed by a third-party confidentiality agreement until such time as the appropriate notice can be given or the appropriate permissions can be obtained. Plaintiff also objects generally to all instructions, definitions, or Interrogatories to the extent they seek disclosure of trade secrets and other confidential research or analyses, development, or commercial information of Plaintiff or any third party.

10. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory is overbroad and unduly burdensome, particularly to the extent they seek "all," "each," or "any" documents, witnesses or facts relating to various subject matters. Fed. R. Civ. Proc. 26(b)(1), (2). To the extent Plaintiff responds to such Interrogatories, Plaintiff will use reasonable diligence to identify responsive documents, witnesses or facts in its possession, custody, or control, based on its present knowledge, information, and belief.

11. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory seeks expert discovery prematurely.

12. Plaintiff objects to any contention Interrogatories in their entirety as premature. Plaintiff will provide its response prior to the close of fact discovery.

13. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory purports to require Plaintiff to restore and/or search data sources that are not reasonably accessible on the grounds that such definitions and Interrogatories would subject Plaintiff to undue burden and expense. Fed. R. Civ. Proc. 26(b)(1), (2).

III. DEFINITIONAL OBJECTIONS.

1. Plaintiff objects to definition number one (1) to the extent it defines "Plaintiff" and "Wikimedia" to include Plaintiff's "parent, subsidiary, and affiliated organizations, and all persons

acting on their behalf, including officials, agents, employees, attorneys, and consultants." Said definition is overly broad, seeks irrelevant information not calculated to lead to the discovery of admissible evidence, seeks information outside of Plaintiff's possession, custody, or control, and would subject Plaintiff to unreasonable and undue annoyance, oppression, burden and expense. Said definition is also vague and ambiguous in that it cannot be determined what is meant by the terms "affiliated organizations" and "all persons acting on their behalf." Plaintiff shall construe "Plaintiff" and "Wikimedia" to mean Wikimedia, and its present officers, directors, agents, and employees.

2. Plaintiff objects to definition number four (4) and to each Interrogatory that purports to require Plaintiff to "state the basis of," "stating the basis of," "state on what basis," or otherwise "state with particularity" or "identify" "all" facts, documents, or persons whose testimony support or dispute any given factual assertion, on the ground that any response thereto would require subjective judgment on the part of Plaintiff and its attorneys, and would further require disclosure of a conclusion or opinion of counsel in violation of the attorney work product doctrine and/or attorney-client privilege. Plaintiff further objects that this definition and all requests to identify documents in the Interrogatories are premature at this early stage of the litigation, would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense, and would impose an obligation to provide information greater than that required by the Federal Rules of Civil Procedure.

3. Plaintiff objects to definition number five (5) as unduly burdensome in that it purports to require Plaintiff to "identify" each "natural person" by providing information including "her most current home and business addresses, telephone numbers, and e-mail addresses, the name of her current employer, and her title."

4. Plaintiff objects to definition number six (6) as unduly burdensome in that it purports to require Plaintiff to "identify" an "entity that is not a natural person" by providing information including "its telephone number and e-mail address, and the full names, business addresses, telephone numbers, and e-mail addresses of both its chief executive officer and an agent designated by it to receive service of process."

5. Plaintiff objects to definition number seven (7) as unduly burdensome in that it purports to require Plaintiff to "identify" documents by providing "(a) the nature of the document (*i.e*, letter, memorandum, spreadsheet, database, etc.); (b) its date; (c) its author(s) (including title(s) or position(s)); (d) its recipient(s) (including title(s) or position(s)); (e) its number of pages or size; and (f) its subject matter," or by providing information in accordance with Defendant's "Specifications for Production of ESI and Digitized ('Scanned') Images attached to Defendant National Security Agency's First Set of Requests for Production." Plaintiff further objects that this definition and all requests to identify documents in the Interrogatories are premature at this early stage of the litigation, would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense, and would impose an obligation to provide information greater than that required by the Federal Rules of Civil Procedure.

IV. INSTRUCTIONAL OBJECTIONS

1. Plaintiff objects to instruction number one (1) to the extent it purports to request "knowledge or information" from Wikimedia's "parent, subsidiary, or affiliated organizations, and their officials, agents, employees, attorneys, consultants, and any other person acting on their behalf." Said request is overly broad, seeks irrelevant information not calculated to lead to the discovery of admissible evidence, seeks information outside Plaintiff's possession, custody, or control, and would subject Plaintiff to unreasonable and undue annoyance, oppression, burden and

expense. Moreover, said request is vague and ambiguous in that it cannot be determined what is meant by the term "affiliated organizations" and "any other person acting on their behalf." Where an Interrogatory requests knowledge or information of Plaintiff, Plaintiff shall construe such request to mean knowledge or information from Wikimedia, and its present officers, directors, agents, and employees.

2. Plaintiff objects to instruction number three (3) as unduly burdensome and imposing an obligation to provide information greater than that required by the Federal Rules of Civil Procedure to the extent it purports to require Plaintiff to "identify each person known by Plaintiff to have such knowledge, and in each instance where Plaintiff avers insufficient knowledge or information as a grounds for not providing information or for providing only a portion of the information requested, set forth a description of the efforts made to locate information needed to answer the interrogatory."

3. Plaintiff objects to instruction number four (4) to the extent it seeks to require it to identify anything other than the specific claim of privilege or work product being made and the basis for such claim, and to the extent it seeks to require any information not specified in Discovery Guideline 10, on the grounds that the additional information sought by Defendant would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense, and constitutes information protected from discovery by privilege and as work product. Plaintiff is willing to discuss acceptable reciprocal obligations for disclosure of information withheld on the basis of attorney-client privilege or attorney work-product.

4. Plaintiff objects to instruction number five (5) to the extent it defines "the time period for which each interrogatory seeks a response" as "the period from July 10, 2008 (the date of enactment of the FISA Amendments Act of 2008, Pub. L. 110-261, 121 Stat. 522) until the date

of Plaintiff's response." This definition is overly broad, seeks irrelevant information not calculated to lead to the discovery of admissible evidence, and would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense. Where appropriate, Plaintiff has defined the specific time period encompassed by specific responses.

5. Plaintiff objects to instruction number six (6) that the Interrogatories are continuing, to the extent said instruction seeks unilaterally to impose an obligation to provide supplemental information greater than that required by Federal Rule of Civil Procedure 26(e) and would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense. Plaintiff will comply with the requirements of the Federal Rules of Civil Procedure and is willing to discuss mutually acceptable reciprocal obligations for continuing discovery.

V. SPECIFIC OBJECTIONS AND RESPONSES TO INTERROGATORIES.

Without waiving or limiting in any manner any of the foregoing General Objections, Definitional Objections, or Instructional Objections, but rather incorporating them into each of the following responses to the extent applicable, Plaintiff responds to the specific Interrogatories in Defendant's Interrogatories as follows:

ALLEGED NSA INTERCEPTION OF SUBSTANTIALLY ALL INTERNATIONAL, TEXT-BASED, INTERNET COMMUNICATIONS

INTERROGATORY NO. 1:

Notwithstanding the holding of the Court of Appeals in this case that "Plaintiffs lack standing to sue … under the Dragnet Allegation because they can't plausibly show that the NSA is intercepting their communications via a dragnet," Wikimedia Found. v. NSA, 857 F.3d 193, 216 (4th Cir. 2017), does Plaintiff still contend, for the purpose of establishing jurisdiction, that NSA Upstream surveillance involves the interception, copying, and review (as those terms are used in paragraph 56 of the Amended Complaint) of all or substantially all international Internet text-based

communications?

RESPONSE TO INTERROGATORY NO. 1:

In addition to the General Objections above which are incorporated herein, Plaintiff also objects that this Interrogatory seeks a statement of Plaintiff's legal strategy or information that is protected by the attorney-client privilege or the attorney work product doctrine. Plaintiff further objects that this Interrogatory is a contention Interrogatory that is premature at this stage in the litigation. Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows: Yes.

INTERROGATORY NO. 2:

Unless Plaintiff's response to Interrogatory No. 1, above, is an unequivocal "no," then please state the basis of Plaintiff's contention that NSA Upstream surveillance involves the interception, copying, and review of all or substantially all international Internet text-based communications, including, but not limited to, the contentions that "Upstream surveillance is intended to enable the comprehensive monitoring of international internet traffic," see Amended Complaint ¶ 48; that "the NSA is temporarily copying and then sifting through the contents of what is apparently most e mails and other text-based communications that cross the border," see id. ¶ 69; that "it would be difficult to systematically search the contents of the communications without first gathering nearly all cross-border text-based data," see Pl.'s Opp. to Defs.' MTD at 18-19; and that the U.S. Government "has acknowledged … that the NSA … examines the full contents of essentially everyone's communications to determine whether they include references to the NSA's search terms," *see id*. at 10.

RESPONSE TO INTERROGATORY NO. 2:

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory is a contention Interrogatory that is premature at this stage in the litigation. Plaintiff further submits that these matters may be the subject of expert testimony, as to which Plaintiff will provide discovery at the appropriate time.

Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery. Plaintiff additionally objects that this Interrogatory is improperly compound in that it contains multiple subparts.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

The bases for Plaintiff's contention include the following:

- Basic principles underlying how Internet communications are transmitted and how surveillance on a packet-switched network operates.
- Privacy & Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of FISA* (2014) ("PCLOB Report"), including pages 7–10, 12–13, 22, 30–41 & n.157, 79, 111 n.476, 120–22, 125, 143, and official government sources concerning Upstream surveillance cited therein.
- [*Redacted*], No. [Redacted], 2011 WL 10945618 (FISC Oct. 3, 2011)
- 50 U.S.C. §§ 1801, 1881a.
- David S. Kris & J. Douglas Wilson, *National Security Investigations and Prosecutions* § 17.5 (July 2015)
- Julia Angwin & Jeff Larson, *New Snowden Documents Reveal Secret Memos Expanding Spying*, ProPublica (June 4, 2015) (and associated documents)

- Julia Angwin et al., *AT&T Helped U.S. Spy on Internet on Vast Scale*, N.Y. Times, Aug. 15, 2015 (and associated documents)
- Julia Angwin et al., *NSA Spying Relies on AT&T's 'Extreme Willingness to Help'*, ProPublica, Aug. 15, 2015 (and associated documents)
- Jeff Larson et al., *A Trail of Evidence Leading to AT&T's Partnership with the NSA*, ProPublica, Aug. 15, 2015 (and associated documents)
- PCLOB, Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 26:15–18 (Mar. 19, 2014) (statement of Robert Litt, General Counsel, ODNI)
- Charlie Savage, *Power Wars* (2015)

Additionally, Plaintiff's contention is based on the principles of Internet communication and the technical necessities of the inspection of Internet communications in transit.

For example, Internet communications in transit are split into packets. Where an eavesdropper is attempting to determine whether the contents of a particular communication in transit on the Internet contain a particular piece of information, the eavesdropper generally must reassemble the packets constituting the communication and then scan the reassembled communication. Reassembling Internet packets requires the temporary copying (or "caching") of those packets until all packets needed for the reassembly have arrived.

Additionally, Upstream surveillance involves the retention of communications that contain targeted selectors. To retain a communication in transit, an eavesdropper must copy and reassemble the packets constituting the communication. But because an eavesdropper cannot know in advance which packets in transit are part of a communication containing a targeted

selector, the eavesdropper must create a temporary copy of all packets that might be a part of such a communication.

The fact that all or substantially all international Internet text-based communications are subject to Upstream surveillance follows necessarily from the information the government has officially disclosed, and it is corroborated by independent news reports. For Upstream surveillance to serve the purposes the government has said it serves, the NSA must be comprehensively monitoring text-based communications originating or terminating in the United States. This is the only way for the NSA to reliably obtain communications to, from, and about its thousands of targets around the world, because those communications travel along paths in and out of the country that are unpredictable and change over time. Moreover, the structure of the Internet backbone facilitates such comprehensive surveillance. Because international communications are channeled through a small number of Internet chokepoints—and because the NSA's own documents show that it is conducting Upstream surveillance at many of those chokepoints—it is straightforward for the government to conduct the comprehensive surveillance necessary for Upstream to function as described.

The government's descriptions of Upstream surveillance make clear that the government is interested in obtaining, with a high degree of confidence, all international communications to, from, and about its targets. For example, the Privacy and Civil Liberties Oversight Board has described the use of Upstream surveillance to collect "about" communications as "an inevitable byproduct of the government's efforts to *comprehensively* acquire communications that are sent to or from its targets." PCLOB Report 10 (emphasis added). And it has said about Upstream surveillance more generally that this method's "success . . . depends on collection devices that can reliably acquire data packets associated with the proper communications." *Id.* at 143 (emphasis

added).

Because the routing of Internet traffic is unpredictable, however, the government can only "comprehensively" and "reliably" obtain communications to, from, and about its thousands of targets by conducting its surveillance on the different routes by which Internet communications enter and leave the country, and by examining substantially all international communications that travel those various routes.

The path that an Internet communication takes is inherently unpredictable. Internet communications are routed around the globe based on a complex set of rules and relationships that are applied dynamically, based on network conditions at any given moment. These network conditions change frequently, and so one cannot know in advance which path a particular communication will travel. Indeed, even the communications between two individuals in a single conversation (such as an Internet chat or email exchange) may take entirely different routes across the Internet backbone, even though the end-points are the same. For example, if an NSA target is having an Internet chat conversation with someone in the United States, the communications *from* the target will frequently follow a different path than those *to* the target. And, of course, a target's location may vary over time. For all these reasons, a target's communications may traverse one Internet circuit at one moment, but a different one later.

The fact that the NSA had, at last public count, 106,469 surveillance targets (some of which are groups with perhaps hundreds or even thousands of members) only reinforces the conclusion that Upstream surveillance of international text-based communications must be comprehensive. *See* ODNI, Statistical Transparency Report Regarding the Use of National Security Authorities for Calendar Year 2016 (Apr. 2017), https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2016. The

communications of so many targets scattered around the world will travel many different routes across the Internet backbone, based on the locations of those various targets, their individual movements over time, and changes in network conditions. These communications will be intermingled with those of the general population in the flow of Internet traffic. An intelligence agency that seeks to reliably intercept communications to, from, or about its targets, could do so only by searching substantially all text-based communications entering or leaving the country.

This allegation is based on the government's official disclosures and on necessary inferences from those disclosures, but it is also corroborated by news accounts. A *New York Times* report from August 2013 states, based on a review of NSA documents and interviews with senior intelligence officials, that "the N.S.A. is temporarily copying and then sifting through the contents of what is apparently most e-mails and other text-based communications that cross the border." Charlie Savage, *N.S.A. Said to Search Content of Messages to and from U.S.*, N.Y. Times, Aug. 8, 2013, http://nyti.ms/1E1nlsi. The same *New York Times* report also explains why the NSA's Upstream surveillance is so far-reaching:

> "Computer scientists said that it would be difficult to systematically search the contents of the communications without first gathering nearly all cross-border text-based data; fiber-optic networks work by breaking messages into tiny packets that flow at the speed of light over different pathways to their shared destination, so they would need to be captured and reassembled."

Id.; see also Charlie Savage, *Power Wars* 207–11 (2015).

Not only does the NSA have an overriding incentive to copy and review substantially all international Internet communications, but the Internet backbone is structured in a way that enables it to do so.

The Internet backbone funnels almost all Internet communications entering and leaving the country through a limited number of chokepoints. The Internet backbone includes a relatively small number of international submarine cables (and a limited number of terrestrial cables) that transport Internet traffic into and out of the United States. Because there are relatively few high-capacity cables carrying international Internet communications, there are correspondingly few chokepoints—*i.e.*, junctions through which all international Internet communications must pass en route to their destinations. By installing its surveillance equipment at the small number of backbone chokepoints, the NSA is able to monitor substantially all text-based communications entering or leaving the United States. And the government has acknowledged that it conducts Upstream surveillance at international links and on the Internet backbone. [*Redacted*], 2011 WL 10945618, at *15; PCLOB Report 36–37.

NSA documents published in the press show that the NSA has installed surveillance equipment at many major chokepoints on the Internet backbone. One of these NSA documents states that the NSA has established interception capabilities on "many of the chokepoints operated by U.S. providers through which international communications enter and leave the United States." *See* Plaintiff's First Amended Complaint ¶ 69. Another shows that just one of those participating providers has facilitated Upstream surveillance at seven major international chokepoints in the United States. *Id.* ¶ 68. Additional reporting states that the NSA has installed surveillance equipment in at least 17 "internet hubs" operated by another major U.S. telecommunications provider. Julia Angwin et al., *NSA Spying Relies on AT&T's 'Extreme Willingness to Help'*, ProPublica, Aug. 15, 2015 (and associated documents).

ALLEGED VOLUME AND GLOBAL DISTRIBUTION OF WIKIMEDIA'S INTERNATIONAL, TEXT-BASED, INTERNET COMMUNICATIONS

INTERROGATORY NO. 3:

Please identify each category of Wikimedia international, text-based, Internet communications that Plaintiff contends, for purposes of establishing jurisdiction, is intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance, including but not limited to, user visits to Wikimedia sites; contributions and edits to Wikimedia websites; Wikimedia discussion forums; Wikimedia discussion pages; e mail sent via Wikimedia among registered users; communications "over wikis" among small or limited groups of users; mailing lists with restricted membership; other use of Wikimedia Projects, websites, and webpages by "community members" to interact with one another; internal log communications; "Community Consultations;" solicitations of user input and preferences; and other communications sent and received by Wikimedia staff in carrying out Wikimedia's work. *See* Amended Complaint ¶¶ 79, 84, 86, 92, 93, 102.

RESPONSE TO INTERROGATORY NO. 3:

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory seeks information that exceeds the scope of jurisdictional discovery as defined by Defendants, *see* ECF No. 116 at 4, and as ordered by the Court.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows. As explained in Wikimedia's First Amended Complaint, Wikimedia contends that Upstream surveillance implicates at least three categories of communications (Am. Compl. ¶ 86): (1) Wikimedia communications with its community members, who read and contribute to Wikimedia's Projects and webpages, and who use the Projects and webpages to interact with each other. Examples of these communications include, but are not limited to, page views to Wikimedia websites, edits and contributions to Wikimedia websites, emails between

registered Wikimedia users and emails on Wikimedia's mailing lists.

(2) Wikimedia's internal log communications.

(3) Electronic communications of Wikimedia staff. Examples of these communications include, but are not limited to, Gmail, Google chat, Internet Relay Chat, and Slack. Additionally, Wikimedia staff members use a variety of third-party tools to conduct their work, including, but not limited to, Google Apps/G Suite, Trello, Sugar, Qualtrics, User Testing and Salesforce.

INTERROGATORY NO. 4:

For each category of Wikimedia international, text-based, Internet communications identified in response to Interrogatory No. 3, above, that Plaintiff contends is intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance, please identify the submarine or terrestrial cables entering or exiting the United States that have carried that category of Wikimedia communications in the past 24 months. To identify a submarine or terrestrial cable means to state its originating or terminating location in the United States, to state its terminating or originating location abroad, and to identify the person(s) owning or controlling it.

RESPONSE TO INTERROGATORY NO. 4:

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory is overbroad and unduly burdensome. Plaintiff further objects that this Interrogatory seeks information that exceeds the scope of jurisdictional discovery as defined by Defendants and as ordered by the Court, and is not reasonably calculated to lead to the discovery of admissible evidence. Specifically, the categories of Plaintiff's communications subject to Upstream surveillance are not relevant to Plaintiff's standing. Plaintiff further objects that this Interrogatory seeks information that is within Defendants' control.

Plaintiff also objects that this Interrogatory is improperly compound in that it contains

multiple subparts. Plaintiff additionally objects that these matters may be the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time.

Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

To a near certainty, Plaintiff's communications traverse all submarine and major terrestrial cables carrying public Internet data into and out of the United States. Publicly available data shows that submarine cables include those listed in Exhibit A. (Exhibit A was created in reliance on publicly available data that Plaintiff has not independently verified.)

INTERROGATORY NO. 5:

For each category of Wikimedia international, text-based, Internet communications identified in response to Interrogatory No. 3, above, that Plaintiff contends is intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance, please identify the Internet circuits entering or exiting the United States that have carried that category of communication in the past 24 months. To identify a circuit means to state its location of entry to or exit from the United States, to state its country (or, if unknown, global region(s)) of origin or termination abroad, and to identify the person(s) owning or controlling it.

RESPONSE TO INTERROGATORY NO. 5:

In addition to the General Objections above which are incorporated herein, Plaintiff also objects that this Interrogatory is overbroad and unduly burdensome. Plaintiff further objects that this Interrogatory seeks information that is not reasonably calculated to lead to the discovery of admissible evidence. Plaintiff further objects that this Interrogatory seeks information that is

within Defendants' control.

Plaintiff also objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff additionally objects that these matters may be the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time.

Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery.

On the basis of these General and Specific Objections, Plaintiff will not provide a response to this Interrogatory.

INTERROGATORY NO. 6:

For each category of Wikimedia international, text-based, Internet communications identified in response to Interrogatory No. 3, above, that Plaintiff contends is intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance, please identify each foreign country to or from which such Wikimedia communications were sent in the past 24 months.

RESPONSE TO INTERROGATORY NO. 6:

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory is overbroad, unduly burdensome and seeks information that is not reasonably calculated to lead to the discovery of admissible evidence. Plaintiff also objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff further objects that this Interrogatory seeks information that exceeds the scope of jurisdictional discovery as defined by Defendants, see ECF No. 116 at 4, and as ordered by the Court.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

(1) Wikimedia communications with its community members. Between April 23, 2017

and December 31, 2017, Wikimedia's U.S. servers received HTTPS requests from, and transmitted HTTPS responses to, users in at least 242 non-U.S. countries, territories and regions. This figure is an estimate that was derived using MaxMind geolocation data to determine the country associated with the client IP of each HTTPS request transmitted to Wikimedia's servers in the United States.

(2) Wikimedia's internal log communications. Every time Wikimedia receives an HTTPS request from a person accessing a Wikimedia Project webpage, it creates a corresponding log entry. Between April 23, 2017 and December 31, 2017, Wikimedia's servers in Amsterdam transmitted over 970 billion logs to Wikimedia's servers in the United States.

(3) Electronic communications of Wikimedia staff. Between January 1, 2015 and December 12, 2017, Wikimedia's office network router located in the United States sent Internet communications to at least approximately 221 non-U.S. countries, territories and regions.

This figure represents Internet outbound communications sent via the following Internet protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

This figure includes communications sent through Wikimedia's Virtual Private Network (VPN).

This figure does not account for the significant number of Internet communications by Wikimedia staff and contractors located internationally, who did not communicate using Wikimedia's Virtual Private Network, but who routinely communicate with Wikimedia staff located at the U.S. headquarters. Between January 1, 2015 and December 22, 2017, Wikimedia engaged over 80 contractors, located across more than 30 different countries.

The results of these analyses will be produced to Defendants. An anonymized list of

Plaintiff's contractors located abroad will also be produced to Defendants.

INTERROGATORY NO. 7:

For each category of Wikimedia international, text-based, Internet communications identified in response to Interrogatory No. 3, above, that Plaintiff contends is intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance, please state the total number of such Wikimedia communications made to and from the United States each year for the years 2008-2017, specifying in each case the manner in which Wikimedia counts the communications in that category (e.g., by site visit, page view, HTTP or HTTPS transmissions, e-mails, other forms of messaging, etc.).

RESPONSE TO INTERROGATORY NO. 7:

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory is vastly overbroad, unduly burdensome and seeks information that is not reasonably calculated to lead to the discovery of admissible evidence. Plaintiff also objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff further objects that this Interrogatory seeks information that exceeds the scope of jurisdictional discovery as defined by Defendants, see ECF No. 116 at 4, and as ordered by the Court.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

(1) Wikimedia communications with its community members. Between April 23, 2017 and December 31, 2017, Wikimedia's U.S. servers received over 500 billion HTTPS requests from users outside of the United States. Each HTTPS request generates a corresponding response; thus Wikimedia exchanged over 1 trillion HTTPS requests and responses with its users between April 23, 2017 and December 31, 2017. These figures are estimates that were derived using MaxMind

geolocation data to determine the country associated with the client IP of each HTTPS request transmitted to Wikimedia's servers in the United States.

(2) Wikimedia's internal log communications. Between April 23, 2017 and December 31, 2017, Wikimedia's servers in Amsterdam transmitted approximately over 970 billion logs to Wikimedia's servers in the United States.

(3) Electronic communications of Wikimedia staff. Between June 4, 2014 and December 12, 2017, Wikimedia's office network router located in the United States made at least approximately 22,934,372 Internet connections to 223 non-U.S. countries, territories and regions.

This figure is an estimate and was derived using a geolocation database that catalogues the IP addresses associated with each country, territory and region for each log entry obtained from the Wikimedia Foundation's office router.

This figure represents the total number of Internet outbound connections sent via the following Internet protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

This figure includes connections sent through Wikimedia's Virtual Private Network (VPN).

This figure does not account for the significant number of Internet communications by Wikimedia staff and contractors located internationally who did not communicate using Wikimedia's Virtual Private Network, but who routinely communicate with Wikimedia staff located at the U.S. headquarters. Between January 1, 2015 and December 22, 2017, Wikimedia engaged over 80 contractors, located across more than 30 different countries.

The results of these analyses will be produced to Defendants. An anonymized list of Plaintiff's contractors located abroad will also be produced to Defendants

INTERROGATORY NO. 8:

For each category of Wikimedia international, text-based, Internet communications identified in response to Interrogatory No. 3, above, that Plaintiff contends is intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance, please state by foreign country the number of such Wikimedia communications made to or from the United States each year for the years 2008-2017, specifying in each case the manner in which Wikimedia counts the communications in that category (e.g., by site visit, page view, HTTP or HTTPS transmissions, e-mails, other forms of messaging, etc.).

RESPONSE TO INTERROGATORY NO. 8:

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory is vastly overbroad, unduly burdensome and seeks information that is not reasonably calculated to lead to the discovery of admissible evidence. Plaintiff also objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff further objects that this Interrogatory seeks information that exceeds the scope of jurisdictional discovery as defined by Defendants, *see* ECF No. 116 at 4, and as ordered by the Court. Plaintiff additionally objects to this Interrogatory as duplicative of other written discovery propounded by Defendants.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

(1) Wikimedia communications with its community members. The number of HTTPS requests that Wikimedia's U.S. servers received from users in each country, territory, or region between April 23, 2017 and December 31, 2017 is attached as Exhibit B and will be included in a forthcoming production to Defendants. Each HTTPS request generates a corresponding response

that is not reflected in the figures included in this analysis. These figures are estimates that were derived using MaxMind geolocation data to determine the country associated with the client IP of each HTTPS request transmitted to Wikimedia's servers in the United States.

(2) Wikimedia's internal log communications. Between April 23, 2017 and December 31, 2017, Wikimedia's servers in Amsterdam transmitted over 970 billion logs to Wikimedia's servers in the United States.

(3) Electronic communications of Wikimedia staff. Between June 4, 2014 and December 12, 2017, Wikimedia's office network router located in the United States sent at least approximately 22,934,372 Internet connections to at least 223 non-U.S. countries, territories and regions. A list of the numbers of these communications broken down by country, territory, or region will be produced to Defendants.

These figures are estimates and were derived using a geolocation database that catalogues the IP addresses associated with each country, territory and region for each log entry obtained from the Wikimedia Foundation's office router.

These figures represent the total number of Internet outbound connections sent via the following Internet protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

These figures include connections sent through Wikimedia's Virtual Private Network (VPN).

These figures do not account for the significant number of Internet communications by Wikimedia staff and contractors located internationally who did not communicate using Wikimedia's Virtual Private Network, but who routinely communicate with Wikimedia staff located at the U.S. headquarters. Between January 1, 2015 and December 22, 2017, Wikimedia

engaged over 80 contractors, located across more than 30 different countries.

The results of these analyses will be produced to Defendants. An anonymized list of Plaintiff's staff and contractors located abroad will also be produced to Defendants.

INTERROGATORY NO. 9:

Please identify the location, by (i) nation, (ii) state, province, or the equivalent, as applicable, and (iii) city, town, or county, as applicable, of each of Wikimedia's servers on which one or more of its "wiki"-based Projects and other related websites and pages (see Amended Complaint ¶ 78), is or since 2008 has been hosted, specifying which of Wikimedia's Projects, sites, or pages is hosted in whole or in part on each server.

RESPONSE TO INTERROGATORY NO. 9:

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory is overbroad, unduly burdensome and seeks information that is not reasonably calculated to lead to the discovery of admissible evidence. Plaintiff additionally objects that this Interrogatory is impracticable in that it requests the identification of each webpage that has been hosted by a particular server. Plaintiff also objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff additionally objects that the term "server" and the phrases "in whole or in part" are vague and ambiguous in the context of this Interrogatory. Plaintiff further objects that this Interrogatory seeks information that exceeds the scope of jurisdictional discovery as defined by Defendants, *see* ECF No. 116 at 4, and as ordered by the Court.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

The following is a list of the locations of each Wikimedia server on which one more of its

"wiki"-based Projects and other related websites and pages is or at some point in time between 2008 and the present has been hosted.

- United States
  - Ashburn, Virginia
  - Carrollton, Texas
  - Chicago, Illinois
  - Dallas, Texas
  - San Francisco, California
  - Tampa, Florida
- The Netherlands
  - Amsterdam, North Holland
  - Haarlem, North Holland
- South Korea
  - Seoul

For purposes of this response, Wikimedia construes the term "server" to mean any public facing Internet access point operated by Wikimedia.

The remainder of this Interrogatory calls for information that exceeds the scope of jurisdictional discovery and Plaintiff therefore will not provide a response at this time.

INTERROGATORY NO. 10:

Please state the number of "logs" or "log entries" (or, if not equivalent, both) contained in each "log communication" sent from Wikimedia servers abroad to Wikimedia servers in the United States, and the frequency with which such log communications are sent. *See* Amended Complaint ¶ 93.

RESPONSE TO INTERROGATORY NO. 10:

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory is vague and ambiguous, overbroad, and not reasonably limited in time. Plaintiff also objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff additionally objects to this Interrogatory as duplicative of other written discovery propounded by Defendants.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

One log or log entry is contained in a single communication. The frequency of log communications transmitted to Wikimedia's servers from outside of the United States is set forth in Plaintiff's response to Interrogatory No. 8.

INTERROGATORY NO. 11:

Please state the basis of Plaintiff's allegations, in paragraphs 61, 85, and 88 of the Amended Complaint, that Wikimedia's alleged "community of volunteers, contributors, and readers consists of individuals in virtually every country on earth" and that Wikimedia "communicate[s] with individuals in virtually every country on earth."

RESPONSE TO INTERROGATORY NO. 11:

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is overbroad and duplicative of other written discovery propounded by Defendants. Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

Numerous facts support Wikimedia's allegations that its "community of volunteers, contributors, and readers consists of individuals in virtually every country on earth" and that

Wikimedia engages in "communications . . . with individuals in virtually every country on earth." As explained in Wikimedia's responses to NSA Interrogatory Nos. 6-8, Wikimedia users from all over the world read and contribute to Wikimedia's Project pages. This analysis is further supported by statistics showing that Wikimedia's Project pages are edited and viewed by millions of users around the world. Wikimedia publishes current monthly page view statistics by country (*available* at https://stats.wikimedia.org/wikimedia/squids/SquidReportPageViewsPerCountryOverview.htm), and maintains an archive with analogous data for past months (*available* at https://stats.wikimedia.org/archive/squid_reports/).

Wikimedia also has dozens of foreign independent but associated entities, including user groups, chapters and thematic organizations. *See* https://meta.wikimedia.org/wiki/Wikimedia_movement_affiliates#chapters.

In the last two years alone, Wikimedia has awarded grants and scholarships to users and programs in dozens of countries. Additionally, Wikimedia projects are currently active in 288 languages, further underscoring Wikimedia's global presence. *See* https://en.wikipedia.org/wiki/List_of_Wikipedias.

INTERROGATORY NO. 12:

Please state the basis of Plaintiff's allegation, in paragraph 61 of the Amended Complaint, that "Plaintiff['s] communications almost certainly traverse every international backbone link connecting the United States with the rest of the world," and the related contention that "Plaintiff['s] communications almost certainly traverse every major internet circuit connecting the United States with the rest of the world," see Pl.'s Opp. to Defs.' MTD at 23, including as part of the response a specification of what Plaintiff means by the term "link" and "circuit" and the

identification by location and ownership or control of each such international backbone link or circuit that Wikimedia communications allegedly traverse.

RESPONSE TO INTERROGATORY NO. 12:

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff further objects that this Interrogatory is a contention Interrogatory that is premature at this stage in the litigation. Plaintiff additionally objects that these matters may be the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time.

Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

The bases of Plaintiff's allegations are the scope and distribution of Plaintiff's international Internet communications.

According to the Foreign Intelligence Surveillance Court and the Privacy and Civil Liberties Oversight Board, Upstream surveillance is directed at "circuits" or "international Internet link[s]" on the Internet backbone. *See* PCLOB, Report on the Surveillance Program Operated Pursuant to Section 702 of FISA 36–37 (2014) ("PCLOB Report"); [*Redacted*], 2011 WL 10945618, at *15 (FISC Oct. 3, 2011). The NSA's Section 702 targeting procedures have similarly described how the NSA targets Internet "links." *See* Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended (July 2009), *available at*

https://www.aclu.org/files/natsec/nsa/20130816/FAA%20Targeting%20Procedures.pdf.

Plaintiff's understanding is that a "circuit" or "link" is a pathway between devices in telecommunications networks. These circuits are carried on, for example, physical media such as cables and fibers, but there is not necessarily a one-to-one correspondence between each circuit and its underlying means of transmission. For example, multiple circuits may traverse a single fiber, and a single circuit may span multiple fibers.

ALLEGATIONS REGARDING NSA INTERCEPTION OF WIKIMEDIA'S INTERNATIONAL, TEXT-BASED, INTERNET COMMUNICATIONS

INTERROGATORY NO. 13:

Please identify each of the international Internet "backbone chokepoints," whether cables, circuits, or other communications facilities, at which Plaintiff contends, in paragraph 66 of the Amended Complaint, the NSA must be conducting Upstream surveillance, stating for each such "backbone chokepoint" the basis of Plaintiff's contention.

RESPONSE TO INTERROGATORY NO. 13:

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff also objects that this Interrogatory seeks information that is within Defendants' control. Plaintiff further objects that this Interrogatory is a contention Interrogatory that is premature at this stage in the litigation. Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

An NSA document states that the NSA has established interception capabilities on "many of the chokepoints operated by U.S. providers through which international communications enter

and leave the United States." *See* NSA Staff Processing Form, Subject: SSO's Support to the FBI for Implementation of their Cyber FISA Orders.

The "chokepoints" at which the NSA conducts Upstream surveillance have included the "seven access sites" identified in an NSA document, reproduced at paragraph 68 of Plaintiff's First Amended Complaint (ECF No. 70-1).

Additional reporting after the filing of the Amended Complaint states that the NSA has installed surveillance equipment in at least 17 "internet hubs" operated by another major U.S. telecommunications provider. *See* Julia Angwin et al., *NSA Spying Relies on AT&T's 'Extreme Willingness to Help'*, ProPublica, Aug. 15, 2015 (and associated documents, one of which describes the surveillance of hundreds of circuits at a specific AT&T trans-Pacific cable site); Julia Angwin & Jeff Larson, *New Snowden Documents Reveal Secret Memos Expanding Spying*, ProPublica, June 4, 2015 (and associated documents); Jeff Larson et al., *A Trail of Evidence Leading to AT&T's Partnership with the NSA*, ProPublica, Aug. 15, 2015 (and associated documents) (describing surveillance on AT&T's network, including on "OC-192 and 10GE peering circuits"; describing surveillance on Verizon's network, including at a cable-landing site called BRECKENRIDGE).

INTERROGATORY NO. 14:

Please state the basis of Plaintiff's allegation, in paragraph 49 of the Amended Complaint, that Upstream surveillance includes a process in which the NSA makes a copy of international text-based communications flowing across certain high-capacity cables, switches, and routers along the Internet backbone.

RESPONSE TO INTERROGATORY NO. 14:

In addition to the General Objections above which are incorporated herein, Plaintiff objects

that this Interrogatory is duplicative of other written discovery propounded by Defendants. Plaintiff additionally objects that these matters may be the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time.

Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

The bases of Plaintiff's allegation are the principles of Internet communication and the technical necessities of the inspection of Internet communications in transit.

For example, Internet communications in transit are split into packets. Where an eavesdropper is attempting to determine whether the contents of a particular communication in transit on the Internet contain a particular piece of information, the eavesdropper generally must reassemble the packets constituting the communication and then scan the reassembled communication. Reassembling Internet packets requires the temporary copying (or "caching") of those packets until all packets needed for the reassembly have arrived.

Additionally, Upstream surveillance involves the retention of communications that contain targeted selectors. To retain a communication in transit, an eavesdropper must copy and reassemble the packets constituting the communication. But because an eavesdropper cannot know in advance which packets in transit are part of a communication containing a targeted selector, the eavesdropper must create a temporary copy of all packets that might be a part of such a communication.

In addition, a *New York Times* report from August 2013 states, based on a review of NSA documents and interviews with senior intelligence officials, that "the N.S.A. is temporarily

copying and then sifting through the contents of what is apparently most e-mails and other text-based communications that cross the border." Charlie Savage, *N.S.A Said to Search Content of Messages to and from U.S.*, N.Y. Times, Aug. 8, 2013; *see* also Charlie Savage, *Power Wars* 207–11 (2015).

INTERROGATORY NO. 15:

Please state the basis of Plaintiff's contentions regarding the manner in which the alleged copying, filtering, and content-review processes referred to in paragraph 49 of the Amended Complaint are carried out.

RESPONSE TO INTERROGATORY NO. 15:

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is a contention Interrogatory that is premature at this stage in the litigation. Plaintiff additionally objects that these matters may be the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time.

Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery. Plaintiff also objects that this Interrogatory is overbroad and duplicative of other written discovery propounded by Defendants.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

The bases of Plaintiff's contentions are the principles of Internet communication and the technical necessities of the inspection of Internet communications in transit.

For example, Internet communications in transit are split into packets. Where an eavesdropper is attempting to determine whether the contents of a particular communication in transit on the Internet contain a particular piece of information, the eavesdropper generally must

reassemble the packets constituting the communication and then scan the reassembled communication. Reassembling Internet packets requires the temporary copying (or "caching") of those packets until all packets needed for the reassembly have arrived.

Additionally, Upstream surveillance involves the retention of communications that contain targeted selectors. To retain a communication in transit, an eavesdropper must copy and reassemble the packets constituting the communication. But because an eavesdropper cannot know in advance which packets in transit are part of a communication containing a targeted selector, the eavesdropper must create a temporary copy of all packets that might be a part of such a communication.

In addition, a *New York Times* report from August 2013 states, based on a review of NSA documents and interviews with senior intelligence officials, that "the N.S.A. is temporarily copying and then sifting through the contents of what is apparently most e-mails and other text-based communications that cross the border." Charlie Savage, *N.S.A Said to Search Content of Messages to and from U.S.*, N.Y. Times, Aug. 8, 2013; *see also* Charlie Savage, *Power Wars* 207–11 (2015).

Other bases of Plaintiff's contentions include:

- The PCLOB Report, including pages 7–10, 12–13, 22, 30–41 & n.157, 79, 111 n.476, 120–22, 125, 143, and official government sources concerning Upstream surveillance cited therein.
- [*Redacted*], No. [Redacted], 2011 WL 10945618 (FISC Oct. 3, 2011)
- 50 U.S.C. §§ 1801, 1881a.
- David S. Kris & J. Douglas Wilson, *National Security Investigations and Prosecutions* § 17.5 (July 2015)

- Julia Angwin et al., *NSA Spying Relies on AT&T's 'Extreme Willingness to Help'*, ProPublica, Aug. 15, 2015 (and associated documents)

- Julia Angwin & Jeff Larson, *New Snowden Documents Reveal Secret Memos Expanding Spying*, ProPublica, June 4, 2015 (and associated documents)

- Jeff Larson et al., *A Trail of Evidence Leading to AT&T's Partnership with the NSA*, ProPublica, Aug. 15, 2015 (and associated documents)

- PCLOB, Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 26:15–18 (Mar. 19, 2014) (statement of Robert Litt, General Counsel, ODNI)

- Charlie Savage, *Power Wars* (2015)

INTERROGATORY NO. 16:

Please state the basis of Plaintiff's allegations in paragraph 59 of the Amended Complaint, including the allegations that "[t]he NSA could readily configure its [alleged] surveillance equipment to ignore" Internet traffic that is "not amenable to … text-based searches;" that such traffic "is likely of no foreign-intelligence interest to the government;" and that "ignor[ing]" such traffic would result in "substantial efficiency gains."

RESPONSE TO INTERROGATORY NO. 16:

In addition to the General Objections above which are incorporated herein, Plaintiff additionally objects that these matters may be the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time.

Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery.

Subject to and without waiving any of these General or Specific Objections, Plaintiff

responds as follows.

Plaintiff's allegations are based on basic principles governing the routing and transmission of Internet communications, as well as basic principles governing how surveillance on a packet-switched network operates.

Plaintiff's allegations are also based on the fact that a substantial percentage of Internet traffic consists of video traffic; and that video traffic from major video-traffic providers, such as Netflix, is likely of little foreign-intelligence interest to the government because it reflects only movie- and television-viewing habits.

INTERROGATORY NO. 17:

Please state the basis of Plaintiff's allegations, in paragraphs 62 and 64 of the Amended Complaint, respectively, that "in order for the NSA to reliably obtain communications to, from, or about its targets in the way it has described, the government must be copying and reviewing all the international text-based communications that travel across a given link," and that "for every backbone link that the NSA monitors using Upstream surveillance, the monitoring must be comprehensive in order for the government to accomplish its stated goals."

RESPONSE TO INTERROGATORY NO. 17:

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff also objects that this Interrogatory is duplicative of other written discovery propounded by Defendants. Plaintiff additionally objects that these matters may be the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time. Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

Plaintiff's allegation is based on basic principles governing the routing and transmission of Internet communications, as well as basic principles governing how surveillance on a packet-switched network operates.

INTERROGATORY NO. 18:

Please state the basis of Plaintiff's allegation, in paragraph 63 of the Amended Complaint, that "[t]o search the contents of any text-based communication for instances of the NSA's 'selectors' as that communication traverses a particular backbone link, the government must first copy and reassemble all of the packets that make up that communication."

RESPONSE TO INTERROGATORY NO. 18:

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory seeks information that is the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time. Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

Plaintiff's allegation is based on basic principles governing the routing and transmission of Internet communications, as well as basic principles governing how surveillance on a packet-switched network operates.

INTERROGATORY NO. 19:

Please state with particularity what Plaintiff means by the term "reliably" as used in

paragraphs 62, 63, and 66 of the Amended Complaint in the phrases "reliably obtain communications," and "reliably intercept … communications," and as the term "reliably," or its equivalent, may be used in Plaintiff's response to any of Defendants' other interrogatories.

RESPONSE TO INTERROGATORY NO. 19:

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is compound, vague, ambiguous and overly burdensome in that it requests that Plaintiff define its use of the word "reliably" in a variety of discrete contexts, and in that it calls for a subjective judgment about what terms are "equivalent" to the term "reliably." Plaintiff additionally objects that these matters may be the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time. Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

The PCLOB has described the use of Upstream surveillance to collect "about" communications as "an inevitable byproduct of the government's efforts to comprehensively acquire communications that are sent to or from its targets." PCLOB Report 10. And it has said about Upstream surveillance more generally that this method's "success . . . depends on collection devices that can *reliably* acquire data packets associated with the proper communications." *Id*. at 143 (emphasis added).

Plaintiff's complaint uses the term "reliably" in different ways depending on context. For example, in paragraphs 62 and 63 of the Amended Complaint, Plaintiff uses the term "reliably" to signify that the government could not conduct Upstream surveillance as it has publicly described

it without undertaking certain steps. Paragraph 66 of Plaintiff's complaint quotes the PCLOB's use of the term "reliably."

INTERROGATORY NO. 20:

Please state the basis of Plaintiff's allegations, in paragraphs 65 and 66 of the Amended Complaint, that in conducting Upstream surveillance "the government's aim is to 'comprehensively' … obtain communications to, from, and about targets scattered around the world," and that "the government is interested in obtaining, with a high degree of confidence, all international communications to, from, or about its targets."

RESPONSE TO INTERROGATORY NO. 20:

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is duplicative of other written discovery propounded by Defendants. Plaintiff also objects that this Interrogatory is improperly compound in that it contains multiple subparts.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

The PCLOB has described the use of Upstream surveillance to collect "about" communications as "an inevitable byproduct of the government's efforts to comprehensively acquire communications that are sent to or from its targets." PCLOB Report 10. And it has said about Upstream surveillance more generally that this method's "success . . . depends on collection devices that can *reliably* acquire data packets associated with the proper communications." *Id*. at 143 (emphasis added); *see also* PCLOB, Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 26:15–18 (Mar. 19, 2014) (statement of Robert Litt, General Counsel, ODNI).

INTERROGATORY NO. 21:

To the extent not already stated or identified in response to Interrogatory Nos. 13-20, above, or in response to Defendant United States Department of Justice's First Set of Interrogatories, Interrogatory Nos. 1-6, please state the basis of Plaintiff's contention that the NSA is intercepting, copying, and reviewing at least some of its communications.

RESPONSE TO INTERROGATORY NO. 21:

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is a contention Interrogatory that is premature at this stage in the litigation. Plaintiff also objects that this Interrogatory seeks information that is the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time. Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery. Plaintiff also objects that this Interrogatory is overbroad and duplicative of other written discovery propounded by Defendants.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

Plaintiff's contention is based on the volume and distribution of its communications, basic principles governing the routing and transmission of Internet communications, and basic principles governing how surveillance on a packet-switched network operates.

Dated: January 11, 2018

/s/Ashley Gorski

Ashley Gorski
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
agorski@aclu.org

Counsel for Plaintiff Wikimedia Foundation, Inc.

No. 20-1191

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

WIKIMEDIA FOUNDATION,

Plaintiff–Appellant,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants–Appellees.

On Appeal from the United States District Court
for the District of Maryland at Baltimore

JOINT APPENDIX—VOLUME 2 OF 7 (JA0920–JA1790)

H. Thomas Byron III
Joseph Busa
Michael Shih
U.S. DEPARTMENT OF JUSTICE
950 Pennsylvania Ave. NW
Washington, DC 20530
Phone: (202) 616-5367
Fax: (202) 307-2551
h.thomas.byron@usdoj.gov

Counsel for Defendants–Appellees

Patrick Toomey
Ashley Gorski
Charles Hogle
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
ptoomey@aclu.org

Counsel for Plaintiff–Appellant
(Additional counsel on next page)

Alex Abdo
Jameel Jaffer
KNIGHT FIRST AMENDMENT INSTITUTE AT COLUMBIA UNIVERSITY
475 Riverside Drive, Suite 302
New York, NY 10115
Phone: (646) 745-8500
alex.abdo@knightcolumbia.org

Deborah A. Jeon
David R. Rocah
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND
3600 Clipper Mill Rd., #350
Baltimore, MD 21211
Phone: (410) 889-8555
Fax: (410) 366-7838
rocah@aclu-md.org

Benjamin H. Kleine
COOLEY LLP
101 California Street, 5th Floor
San Francisco, CA 94111
Phone: (415) 693-2000
Fax: (415) 693-2222
bkleine@cooley.com

***Wikimedia Foundation v. National Security Agency, et al.*,**
No. 20-1191 (4th Cir.)

JOINT APPENDIX
Table of Contents

VOLUME 1

Exhibits to Wikimedia Foundation's Motion to Compel

Exhibits to Defendants' Opposition to Wikimedia Foundation's Motion to Compel

Exhibits to Wikimedia Foundation's Reply in Support of Its Motion to Compel

Opinion & Order Denying Wikimedia Foundation's Motion to Compel

Exhibits to Defendants' Motion for Summary Judgment

VOLUME 2

Exhibits to Wikimedia Foundation's Opposition to Defendants' Motion for Summary Judgment

VOLUME 3

Exhibits to Wikimedia Foundation's Opposition to Defendants' Motion for Summary Judgment (Cont'd)

VOLUME 4

Exhibits to Wikimedia Foundation's Opposition to Defendants' Motion for Summary Judgment (Cont'd)

VOLUME 5

Exhibits to Wikimedia Foundation's Opposition to Defendants' Motion for Summary Judgment (Cont'd)

VOLUME 6

Exhibits to Defendants' Reply in Support of Their Motion for Summary Judgment

VOLUME 7

Exhibits to Wikimedia Foundation's Sur-reply in Opposition to Defendants' Motion for Summary Judgment

Exhibits to Defendants' Sur-reply in Support of Their Motion for Summary Judgment

Opinion & Order Granting Defendants' Motion for Summary Judgment

Wikimedia Foundation's Notice of Appeal

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 1

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, *Plaintiff*, v. NATIONAL SECURITY AGENCY / CENTRAL SECURITY SERVICE, *et al.*, *Defendants*.	No. 1:15-cv-00662-TSE

DECLARATION OF SCOTT BRADNER

I. INTRODUCTION

1. My name is Scott Bradner. I have been asked by the plaintiff's counsel in *Wikimedia Foundation v. National Security Agency*, No. 1:15-cv-006622-TSE (D. Md.), to provide an expert report addressing the following questions:

   a. What is the basic structure of the Internet and how do communications traverse it?

   b. How does upstream collection work, based on official government acknowledgments and my expertise in network design and operation?

   c. What is the likelihood that the government has copied and reviewed the plaintiff's international text-based Internet communications in the course of upstream collection?

2. In this declaration I will address these questions based on my own technical expertise and experience, and on relevant technical principles. The information I used to understand and explain the Section 702 collection of Internet transactions came from my review of documents provided to me by plaintiff's counsel. Counsel has informed me that all of the U.S. government documents they provided have been officially released by the government.

3. A list of the documents provided to me by plaintiff's counsel is attached as Appendix B.

4. After explaining my conclusions, I address the declaration of Dr. Henning Schulzrinne, filed in support of the government's motion for summary judgment.

5. In this declaration, I refer to actions such as copying, reassembling and reviewing as if they were wholly performed by the NSA. But in doing so, I am specifically including the possibility that some or all of those actions are performed by

others at the direction of the NSA. In addition, when I refer to "copying," as in "copying a packet," I am including any process which results in one or more duplicate copies of the original packet, for example, splitting a beam of light and reconstructing packets from each portion of the split light beam, as well as using an electronic device to produce a copy of a packet it received on a network.

II. SUMMARY OF MY CONCLUSIONS

6. After reviewing the materials available to me in this case I have concluded the following. These conclusions apply both before and after the "about" collection was stopped:

a. It is my opinion that, to conduct upstream collection of international Internet communications traversing any particular circuit, as this operation has been described by the government, the NSA must be copying at an absolute minimum the packets constituting the transactions it wishes to review for the presence of selectors. Based on other practical necessities I describe below, it is also my opinion that the NSA is almost certainly either (1) copying all packets traversing that circuit or (2) copying all of the packets that an IP address filter test determines are not part of a wholly domestic transaction.

b. It is my opinion that, in order to review Internet transactions to determine if a selector tasked for collection is present, the NSA must be reassembling the packets of the transactions it intends to review.

c. It is my opinion that the NSA must review the reassembled Internet transactions in order to identify those that include a tasked selector and thus are subject to collection under the upstream collection program.

d. It is my opinion that it is virtually certain that Wikimedia's international communications traverse every circuit carrying public Internet traffic on every international cable connecting the U.S. to other countries.

e. It is my opinion that it is virtually certain that the NSA has, in the course of the upstream collection program, copied, reassembled and reviewed at least some of Wikimedia's communications.

7. I have carefully reviewed the declaration of Dr. Schulzrinne, and nothing in it alters the above conclusions. I will address parts of his declaration at various places in my declaration and more fully at the end of my declaration. In summary, I conclude as follows:

a. Dr. Schulzrinne does not directly address the likelihood that the NSA has, in the course of the upstream collection program, copied, reassembled and reviewed at least some of Wikimedia's communications. Accordingly, he does not deny that it is virtually certain that the NSA has, in fact, done so.

b. Dr. Schulzrinne speculates that the NSA could, in theory, have designed its upstream collection program to have avoided the copying, reassembly and review of *any* of Wikimedia's communications, but as I explain in detail below, his speculation is technically inaccurate and it is, as a practical matter, simply implausible that the NSA designed and operated its upstream collection program as Dr. Schulzrinne speculates it could have to avoid such copying, reassembly and review. For example, he speculates that the NSA could have been and is "blacklisting" Wikimedia's IP addresses or could have been and is filtering out all web traffic from upstream collection. Blacklisting

Wikimedia's IP addresses would not in fact avoid the copying, reassembly or review of Wikimedia's communications, as I explain below. Moreover, there is no reason to believe that the NSA has been or is currently attempting to filter out Wikimedia's traffic, and there are compelling reasons to believe that it isn't. Finally, it strains credulity to suggest that the NSA is, in the course of an Internet surveillance program, deliberately filtering out all *web activity*, one of the most common modes of communication on the Internet. (The NSA has in any event confirmed that it monitors web activity under upstream collection, as I note below.)

c. For these reasons, Dr. Schulzrinne's speculation about technically possible but exceedingly unlikely measures the NSA might have been taking or might currently be taking to avoid Wikimedia's communications do not alter my conclusion that it is a virtual certainty that the NSA has, in the course of the upstream collection program, copied, reassembled and reviewed at least some of Wikimedia's communications.

8. I rely on my own knowledge as well as public technical publications for the background of the technology section and on the documents supplied to me by Wikimedia's counsel to understand the NSA's upstream collection program and to support these opinions.

III. QUALIFICATIONS

9. My background and expertise that qualify me as an expert in the technical issues in this case are as follows:

A. Employment

10. I worked at Harvard University ("Harvard") in a number of information technology roles, from 1966 to 2016, at which time I retired. My last role at Harvard was as a Senior Technology Consultant in the office of the Harvard University Chief Technology Officer (CTO) where I worked on identity management projects. Before joining the Harvard CTO's office I was the Harvard University Technology Security Officer (UTSO) for 8 years. I currently teach courses on *Technology, Security, Privacy, and the Realities of the Cyber World* at the Harvard University Extension School and have supervised masters and Ph.D. theses for students in Harvard University itself and in the Harvard University Extension School. In the past I have taught classes for undergraduate and graduate students at Harvard University and multi-day tutorials in the 1990s to thousands of students at the largest U.S. Internet-related trade show as well as at a number of major technology companies including IBM, Oracle and Nortel. I have also consulted for many technology companies, a number of universities and for multiple departments within the U.S. government.

B. Publications

11. I have authored or co-authored 4 books and over 90 articles or other publications in peer-reviewed journals, conference proceedings, popular publications, monographs and standards organizations. These publications span a range of topics including analyzing network hardware, Internet technology, technology policy and standards processes. In addition, between 1992 and 2013 I wrote a regular column in the technical journal *Network World*, which was read around the world.

C. The Internet Engineering Task Force

12. The Internet Engineering Task Force (IETF) is a primary standards creation and maintenance body for the Internet. The work of the IETF is conducted in Working Groups and IETF Working Groups are organized into Areas. Each of the technical areas in the IETF is managed by one to three Area Directors. At various times I served as the Director or co-Director of the IETF's Operational Requirements, Operations and Management, IP Next Generation, Transport and Sub-IP areas. As an Area Director, I served as one of the members of the Internet Engineering Steering Group (IESG), the IETF's standards approval and general management committee from 1993 to 2003. As a member of the IESG, I reviewed and evaluated hundreds of IETF working documents that were proposed by IETF working groups or IETF participants to be approved as IETF standards. The documents I was involved in approving covered all areas of IETF technology and included all aspects of Internet design, operation and evolution. I will note in passing that I worked often with Dr. Schulzrinne in the IETF.

D. Involvement in Data Network Design and Operation

13. I was involved in the design, operation and use of data networks at Harvard University since the early 1970s, and was involved in the design, implementation and operation of the original Harvard data networks, the Longwood Medical Area network (LMAnet) and the New England Academic and Research Network (NEARnet).

14. Additionally, I was the founding chair of the technical committees of LMAnet, NEARnet and the Corporation for Research and Enterprise Network (CoREN). I was involved in the day-to-day operation of these networks as well as their evolution.

15. I have also served as a consultant on network design, management and security to educational institutions, federal agencies, international telecommunications enterprises and commercial organizations ranging from Fortune 500 companies to small businesses, from 1989 to the present. I have served as an expert witness in the Communications Decency Act challenge (*Reno v. ACLU*, 521 U.S. 844 (1997)) in U.S. federal court and in a number of patent cases.

16. In addition, I have also served on the technical advisory boards of about two-dozen companies in various technology fields, mostly relating to the Internet and other data networks, and I have been a frequent speaker at technical conferences.

17. My CV and list of previous cases is attached to this declaration as Appendix A.

E. Compensation

18. I am not being compensated for my work in this case other than for travel expenses, if any.

IV. BACKGROUND OF THE TECHNOLOGY IN THIS CASE

19. I agree in general with the background information Dr. Schulzrinne provides in ¶¶ 16-44 of his declaration. I note below where we disagree. The following involves more detail and sometimes a different focus from Dr. Schulzrinne's background section.

20. This case involves communications over the Internet. The Internet is the world-wide collection of interconnected networks that operate following the standards that define the Internet Protocol. The different networks that make up the Internet are operated independently. There is no overall manager of the Internet, nor is there any general form of governance of the Internet. The Internet operates by mutual agreement

among the companies that produce the computers that connect to the Internet and the companies that operate the independent networks that make up the Internet to implement the same set of technical standards in the software of the computers and to operate the networks in ways that are consistent with generally ad-hoc operational standards. See below for a fuller description of the Internet.

21. To put the relevant technologies and concepts in context, I will provide a brief history of the Internet, define some of the terms I will be using, explain the key protocols in use on the Internet today, and describe other key features of the Internet and its architecture relevant to this case.

A. History of the Internet

22. I will now provide a short history of the Internet as a way to introduce the technology of the Internet that is relevant to this case.

1. Pre-1960s

23. The wiring of the world started with the Samuel Morse patent for the telegraph in 1847 and accelerated with the Alexander Graham Bell telephone patent in 1876. Until the late 1960s the networks that supported the telegraph and telephone services only supported those services—that is, they were specific-purpose not general-use networks. In describing the environment that led to the Internet, I will focus on the telephone network.

24. By the beginning of the 1960s, telephone networks had evolved into a general hierarchical hub-and-spoke architecture. The telephones in an area, for example a town, were connected to a telephone switch in a local central telephone office in that town with dedicated pairs of wires. As many as tens of thousands of telephones could be connected to each of these local central telephone switches. These local central office

telephone switches were connected to a more central telephone switch, which, in turn, was connected to an even more central switch.

25. To make a telephone call, a caller would dial a telephone number. The telephone number was sent, digit-by-digit, to the local central office telephone switch over the dedicated pair of wires. Using this telephone number, the local central office switch would then cause a dedicated path to be set up between itself and the local central office telephone switch connected to the telephone assigned the telephone number the caller had dialed. The path might traverse a number of telephone switches. The dialed telephone would then ring and, if someone picked up the dialed phone, a conversation could be held over the dedicated path. When the caller or called person hung up, the dedicated path established to support the call would be "torn down"—that is, the individual wires that had been used to make up the path would be released to be used for future telephone calls.

26. Two significant limitations of this telephone system architecture included:

a. That the wire between the telephone and the local central office telephone switch could only be used for one thing, a single telephone call, at a time.

b. That the failure of a telephone switch or of a connection between pairs of telephone switches would terminate all telephone calls whose paths went through the switch or link that failed.

2. Advanced Research Projects Agency (ARPA)

27. Parallel developments in the Cold War between the U.S. and the Soviet Union set the stage for the development of the modern Internet. In the 1950s and 1960s, in that context, the launch of the Sputnik spacecraft by the Soviet Union on October 4, 1957 was a profound shock to the U.S. scientific and political establishment. In direct

response to the launch of the Sputnik, President Dwight David Eisenhower established the Advanced Research Projects Agency (ARPA) in the U.S. Department of Defense within three months of the launch. ARPA was established with a very broad mandate to undertake advanced research in any area that might be helpful to the U.S. military and, hopefully, to minimize the chance of another Sputnik-like surprise. ARPA came to play an important role in the development of the Internet.

3. The origin of Packet Data Networks

28. ARPA was not alone in supporting advanced research within the U.S. Department of Defense. Relevant to this history, the U.S. Air Force supported research efforts at RAND Corporation. One of the researchers at RAND was Paul Baran. Mr. Baran was very worried about the survivability of the telephone system that the U.S. military would need to use for communication in the aftermath of a nuclear attack on the U.S. Mr. Baran developed an alternative architecture that would have a much better chance of surviving mass destruction. That alternative architecture became the basis of today's Internet.

4. Packets

29. As noted above in ¶ 26, one of the issues with the architecture of the telephone system in the 1960s was that the failure or destruction of a single one of the large telephone switches or links between switches would terminate any call currently running though that switch or link. Mr. Baran developed the idea of using a large number of small switching nodes interconnected by links as a redundant array. The switching systems are represented by the dots and the links by the interconnecting lines in the sample distributed network shown in the figure below from Mr. Baran's 1962 paper *On Distributed Communications Networks*:

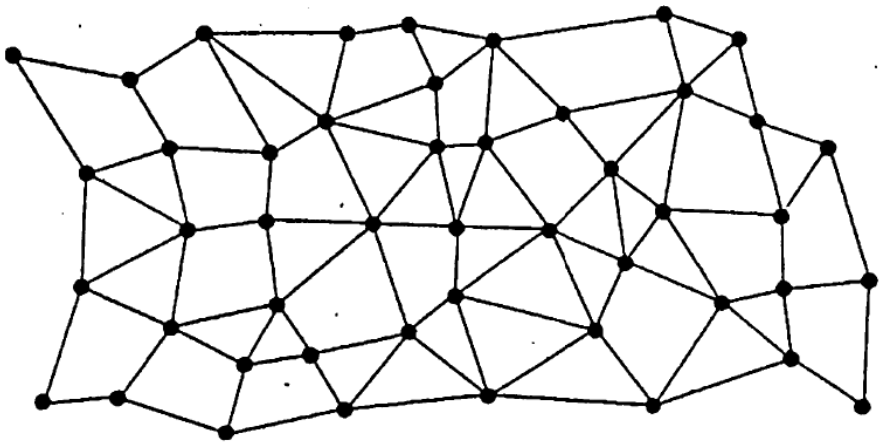


Figure 1[1]

30. With this type of redundant architecture, connections can get rerouted in case of a failure of a link or of a switching node. The following figure shows a sample path (green line) that could be used through a network. The path traverses a number of switching nodes and links:

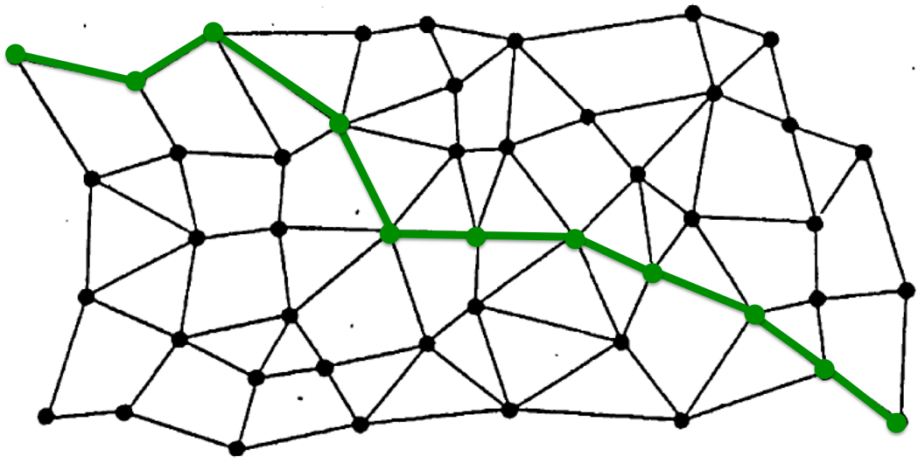


Figure 2

[1] Appendix G at 5 (Paul Baran, RAND Corp., *On Distributed Communications Networks* at 4 (Sept. 1962)).

31. The following is the same network showing a sample path after the failure of a switching node in the network (marked by the red X).

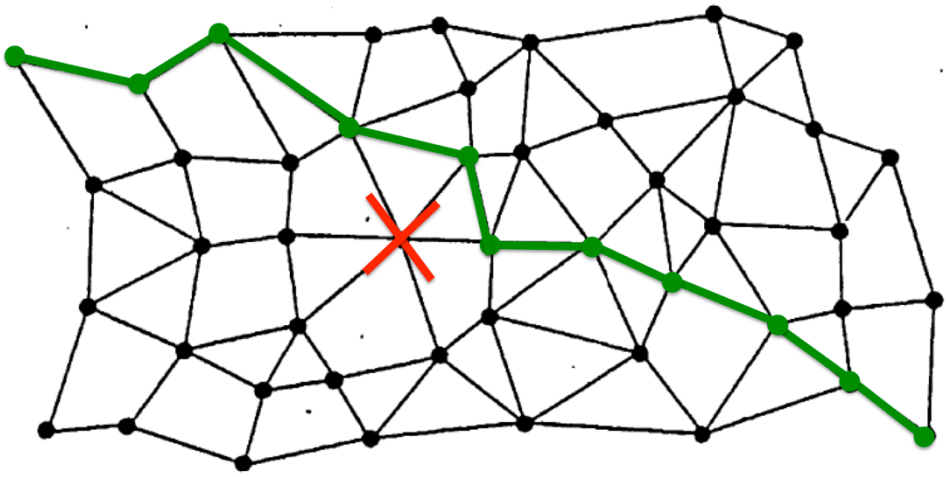


Figure 3

32. But redundancy, by itself, is not sufficient. A communication, such as a voice call, would be disrupted during any reroute of the communication path. So Mr. Baran developed the concept of breaking each communication up into multiple autonomous chunks, which he called message blocks but which are now known as "packets", the term which I will use in this report. Mr. Baran's diagram of a packet is shown in the following figure from his 1962 paper:

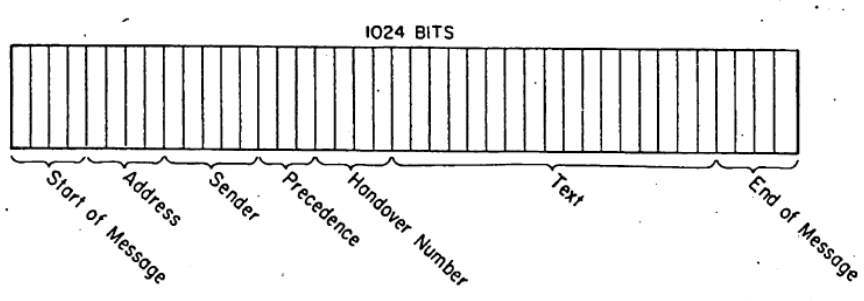


Figure 4[2]

33. Each of the packets includes a field at the start of the packet that tells the network to which network node this packet is to be delivered (the "Address" field), a field that says what network node sent the packet (the "Sender" field), some other control information (the "Precedence" and "Handover Number" fields) and a payload field which contains the chunk of information being transported in the packet (the "Text" field).

34. These same types of fields are present in the packets that traverse today's Internet. For example, the following figure shows the format of an Internet Protocol version 4 (IPv4) packet:

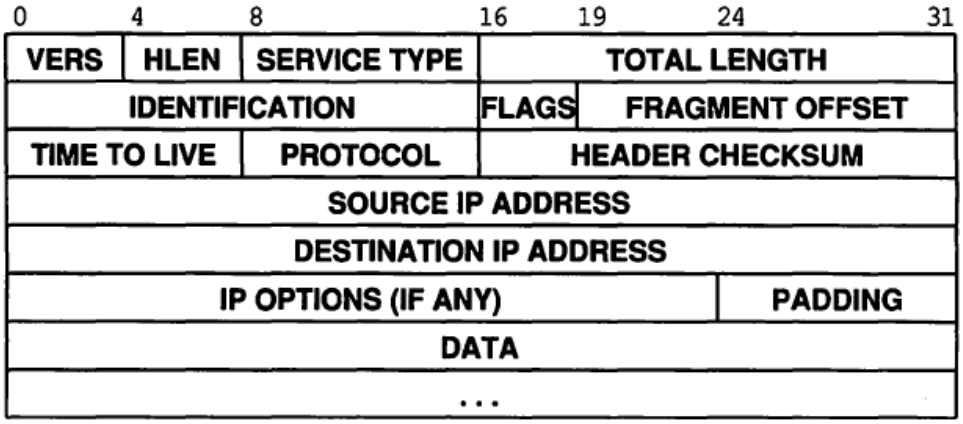


Figure 5 — IP packet format[3]

35. IPv4 is the version of the Internet Protocol (IP) that was deployed in 1983 and is still the predominant version in use today. A revised version of IP, known as IPv6, is being deployed but is not yet in general use. The IPv4 and IPv6 headers differ but not in ways that alter this discussion.

[2] Appendix G at 27 (Baran, *supra* note 1, at 26).

[3] Douglas E. Comer, *Internetworking with TCP/IP: Principles, Protocols, and Architecture* (2nd ed. 1991).

36. The figure above shows a "source IP address" field (Baran's "sender" field), a "destination IP address" field (Baran's "address" field), a number of fields that correspond to Baran's control information (e.g., "service type", "protocol", etc.) and a "data" field (Baran's "text" field). (See ¶¶ 95-104 for a fuller discussion of the Internet Protocol.)

37. Breaking the communication into packets means that only a small part, if any, of the communication will get lost, and perhaps have to be retransmitted, if the path is disrupted by some failure rather than having the whole communication be terminated.

38. Another big advantage of using packets to carry communications is that multiple communications can be run over the same link at the same time by intermingling packets from different communications. Many, even hundreds or thousands, of separate communications can be running over a single link at the same time, and if the link is in the center of a network, such as the network shown in the Baran figure, these communications can be to and from many different sending and receiving nodes.

5. The ARPANET

39. Meanwhile, back at ARPA, there was an interest in sharing big research computers among multiple researchers located around the country or even outside of the country. At that time computers that were needed for large-scale computation were physically very large and very expensive—much too expensive for the government to be able to provide a computer for each research institution. Thus ARPA had an interest in making it possible for researchers at different locations to be able to share the use of the large computers.

40. The approach ARPA decided to take was to build a nation-wide network to interconnect the big computers and the institutions where the researchers were located. ARPA also decided to use the basic concepts that Mr. Baran had developed, even though ARPA at that time was more interested in sharing computing resources than surviving nuclear attacks. The same technology, packet-based data networking, would support both types of needs.

41. The initial parts of the resultant network, known as the ARPANET, were installed in four locations on the U.S. west coast in late 1969. Within a few years the network had been extended to the U.S. east coast and to dozens of nodes. A few years later there were a few hundred ARPANET nodes including a few in the U.K. and Europe.

42. The original ARPANET design had a significant limitation. The ARPANET operated using the Network Control Protocol (NCP). NCP was designed to interconnect network nodes, generally a single node at a location such as a university but occasionally two or three. Bob Kahn realized that, in order to be able to grow, the design had to be changed such that the ARPANET would interconnect networks rather than nodes. Each location, such as Harvard, could have its own network with as many nodes as it wanted to have. The nodes on the networks at multiple sites could then communicate with nodes at other sites with an almost unlimited ability to grow the number of nodes.

43. Dr. Kahn enlisted the help of Dr. Vint Cerf, and together they developed the Internet Protocol. IP defines a way to interconnect networks (thus “inter-net”) such that a node on one network can communicate with another node on the same network or with a node on a different network. The Internet Protocol specifications define the

format of Internet Protocol packets, and, in a general way, how packets are constructed, transported and processed.

44. The ARPANET transitioned from NCP to the Internet Protocol starting on January 1, 1983. This was the start of the Internet, as the concept is understood today.

45. ARPA operated the ARPANET as a backbone network—i.e., a network that interconnected other networks—until 1990. Note that the ARPANET did not have a single link that was its backbone carrying all of its traffic. Instead, as shown in Figure 6 from October 1980, the ARPANET, like Internet Service Providers these days, had a mesh-like set of links that provided for redundancy and shared the traffic load. Traffic would only traverse as much of the ARPANET links as it needed to in order to reach its destination.

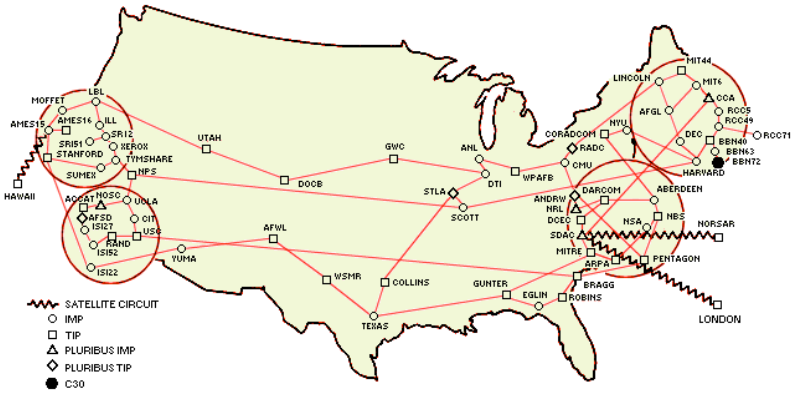


Figure 6 — The ARPANET in October 1980[4]

46. By the time ARPA shut down the ARPANET, the U.S. National Science Foundation (NSF) was operating its own backbone network (NSFNET) to interconnect networks at NSF-sponsored universities and research centers. The NSF replaced the ARPANET until the NSFNET was closed down in 1995.

[4] *Internet Technology*, Technology UK, http://www.technologyuk.net/telecommunications/internet/internet-technology.shtml.

47. Starting in the late 1980s, commercial Internet service providers operating in parallel to the NSFNET began to appear. By the mid-1990s there were thousands of small local ISPs and a growing number of nation-wide ISPs. By the end of the 1990s, a few of the U.S. ISPs had expanded internationally.

B. Definitions

48. The Internet today remains a packet data network, following Baran's original concept of redundant network connections and autonomously routed chunks of data called packets. Before explaining the key protocols and architecture of the Internet today, I will first specify what I mean by the terms that I will be using in this report. Unless otherwise noted, these definitions are widely accepted and consistent with the use of these terms by experts in the field of Internet communications and architectures.

1. A Communication

49. The term ***communication*** does not have a single precise definition in the field of Internet communications, but in the context of this report I will generally use the term "communication" to mean data exchanged between a pair of nodes on a network. Communications include phone calls, email messages, data files, requests for web pages and web pages. Communications are broken up into chunks, called ***packets***, for transmission over the network. Communications are bidirectional with packets flowing in both directions even when a user is viewing a web page.

2. Layers, links and nodes

50. Networks are organized into ***layers*** to simplify design and operation. Each layer provides services to the layer above it and shields the layer above it from the complexities of providing that service. The Internet follows the 4-layer model shown in the following figure:

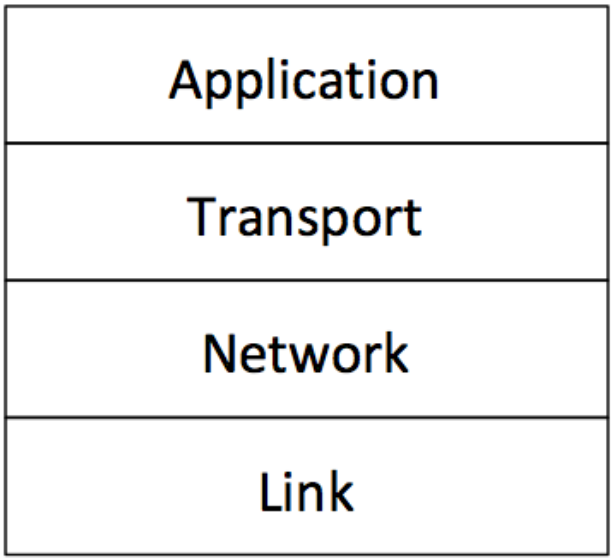


Figure 7 — Internet 4-layer model

51. The above figure is consistent with the description in ¶ 27 of Dr. Schulzrinne's report except that he includes the physical network that the packets ride on as a layer below the data-link layer.

52. The ***Link Layer***, also known as the ***Data-Link Layer***, is responsible for delivering data in the form of packets over a physical or virtual network link between network devices. A ***physical network link*** is a direct connection between two network devices using a physical medium such as copper wire or fiber optic cable. Another type of network link I will mention later is a virtual network link. A ***virtual network link*** appears to the two nodes communicating over the virtual link to be a physical network

link, but the virtual network link is not restricted to being a physical connection just between the two nodes. Instead it can be implemented as a continuous communication over a network consisting of multiple physical network links. See, for example, the discussion of ***tunnel*** below.

53. One example of a physical network link is Ethernet, the most common type of physical network link used in enterprise data networks. Another example is WiFi, a radio-based equivalent of Ethernet used with portable network devices such as laptops and smartphones. A third example is fiber-optic cable. Short fiber-optic cables are used between buildings in a campus network, longer ones are used between cities and very long fiber-optic cables are used to interconnect continents. A fiber-optic cable contains multiple individual optical fibers. Each individual fiber in a fiber-optic cable can be used as a network link, or individual fibers can be divided up into many different colors of light, known as ***lambdas***. An individual lambda can be used as a network link or multiple lambdas can be combined into a network link.

54. Those network links, such as Ethernet and WiFi, which can interconnect more than two network devices, make use of ***link-layer addresses*** to specify the source and destination of the packets making up communications running over the link-layer network. A link-layer address is a numerical value that uniquely identifies a node on a particular network. The network links that only interconnect two devices, such as lambdas in an optical fiber, generally do not need such addresses since there is only one possible source and one possible destination on any particular link.

55. Sets of interconnected network links are often referred to as ***Local Area Networks*** (***LANs***). If a LAN consists of more than a single network link, the individual

network links in the LAN are interconnected with switches. See below for a description of switches.

56. The ***Network Layer*** is responsible for delivering data between network devices on different LANs. The Internet Protocol defines the network layer in the Internet. See ¶¶ 94-104 for more information about IP. The network layer uses network addresses, rather than link-layer addresses to specify the source and destination of the packets running over a network layer network. A ***network address*** is a numerical value that uniquely identifies a node on a particular network. If the network is the Internet, the network address must be unique across the Internet. The network addresses used in the Internet are ***Internet Protocol (IP) addresses***. See below in ¶¶ 97-98 for a discussion of IP addresses.

57. Devices on the Internet normally have both a link-layer and network address. The link-layer address is used to deliver the packet to the correct device on a particular LAN, and the network address is used to get the packet to the correct LAN. I will describe this further below.

58. The Internet is composed of LANs interconnected with routers. See below in ¶¶ 84, 86 for a description of routers.

59. The ***Transport Layer*** is responsible for managing the flow of packets in each direction that make up a communication between two network devices. As part of this function the transport layer is responsible for splitting the data into packets for transmission and reassembling them into continuous data when they are received. The Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) are the two

most common transport layer protocols used in the Internet. See the discussions on TCP (¶¶ 110-115), flows (¶ 62) and packets (¶¶ 74-82) below.

60. The ***Application Layer*** is responsible for handling an Internet data flow in a way defined for the specific application the flow is a part of. Applications are the way that people use the Internet. Internet applications most relevant to this case include electronic mail (email) and the world wide web. See below for discussions of these Internet applications.

61. Portions of every packet transferred across the Internet provide support for each of the above layers. See the description of a packet below in ¶¶ 74-82.

3. Flow

62. A ***flow*** is a set of packets that are part of a single communication and that are transported from one network node to another network node. While communications are generally bidirectional, flows are unidirectional. The packets that make up a flow are distinguished from other packets when the following five fields in a packet are identical between the packets: the source and destination IP addresses, the protocol field and the source and destination port numbers. This information is often called a ***five tuple*** (or ***5-tuple***). See below for a discussion of packets that includes a discussion of these fields.

4. Transaction

63. The government's response to the Foreign Intelligence Surveillance Court's Briefing Order of May 9, 2011 defines ***transaction*** as follows:

> *a complement of 'packets' traversing the Internet that together may be understood by a device on the Internet and, where applicable, rendered in an intelligible form to the user of that device.*[5]

64. The government's use of the term "transaction" is not a common way that the term is understood in Internet communications. Merriam-Webster's definition of "transaction" relating to communications is the more common understanding:

> *a communicative action or activity involving two parties or things that reciprocally affect or influence each other.*[6]

65. But I will adopt the government's definition for the term "transaction" for this report where the term is used in regards to upstream collection. In practice, a "transaction", as defined by the government, appears synonymous with a "flow" as I define the term above in ¶ 62.

66. The NSA also talks about ***multi-communication transactions*** (***MCTs***), which contain more than one individual communication, such as more than one email message, not all of which would be proper candidates for collection on their own:

> *NSA Defendants respond that to their understanding (i) the term "single communication transaction," when used in reference to Upstream Internet collection, meant in unclassified terms an Internet transaction that contained only a single, discrete communication, and (ii) the term "multi-*

[5] Appendix C at 1 (FISC Submission (June 1, 2011)).

[6] *Transaction*, Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/transaction.

> *communication transaction" meant, in unclassified terms, an Internet transaction that contained multiple discrete communications.*[7]

67. The NSA says that an MCT might consist of, for example, multiple email messages.[8]

68. The NSA says that it is not technically feasible to only collect the individual transactions in an MCT that qualify for collection under the upstream collection program:

> *The NSA's acquisition of MCTs is a function of the collection devices it has designed. Based on government representations, the FISC has stated that the "NSA's upstream Internet collection devices are generally incapable of distinguishing between transactions containing only a single discrete communication to, from, or about a tasked selector and transactions containing multiple discrete communications, not all of which are to, from, or about a tasked selector."*[9]

69. Also see below at ¶¶ 316-320.

5. Network

70. A ***network*** consists of a set of computers and the network links and routers and switches that permit the computers to exchange communications. The Internet is a network of networks.

[7] Appendix D at 13 (NSA Response to Plaintiff's Interrogatory No. 8 (Dec. 22, 2017)).

[8] Appendix E at 15-16 n.17 (FISC Opinion (Apr. 26, 2017)).

[9] Appendix F at 45 (Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of FISA* at 40 (July 2, 2014) ("PCLOB Report")).

6. Network Node

71. A ***network node*** is a computer connected to a network. Network nodes include the ***end-systems*** between which communications are exchanged and the network nodes (such as switches and routers) that forward the packets that make up a communication between the end-systems. Such end-systems include user desktop or laptop computers and smartphones as well as computers that provide services to the users such as web servers—for example www.cnn.com and www.wikipedia.org.

7. Circuit

72. In its response to one of Plaintiff's interrogatories, the NSA described a ***circuit*** as follows:

> *NSA Defendants respond that to their understanding a "circuit," within the context of Internet communications, traditionally consists of two stations, each capable of transmitting and receiving analog or digital information, and a medium of signal transmission connecting the two stations. The medium of signal transmission can be electrical wire or cable, optical fiber, electromagnetic fields (e.g., radio transmission), or light. Individual circuits may be subdivided further to create multiple "virtual circuits" through application of various technologies including but not limited to multiplexing techniques.*[10]

73. This description is consistent with the definition for "network link" I provided above in ¶¶ 52-55, with the addition of the nodes at each end of the link. I will adopt the government's definition of circuit for the purpose of this report.

[10] Appendix D at 6 (NSA Response to Plaintiff's Interrogatory No. 2 (Dec. 22, 2017)).

8. Packet

74. A ***packet*** is a chunk of a communication. Packets in the Internet can vary in size and are autonomous, meaning that they can be processed independently by devices within the network (explained below). An example Internet packet is shown in the following figure. As explained below, each layer in this figure depicts the corresponding layer within the four-layer model of the Internet, described above in ¶¶ 50-61:

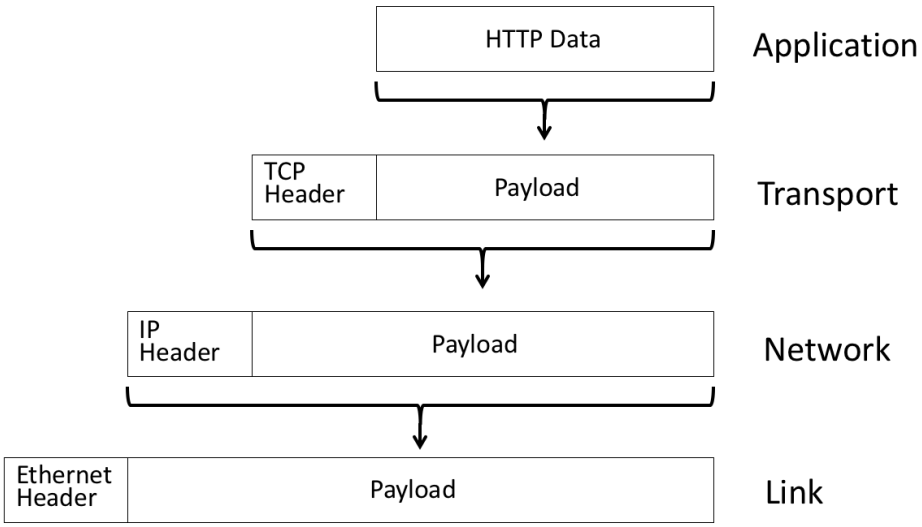


Figure 8 — Packet format showing web data over Ethernet

75. Figure 7 shows an Internet packet as I described above in the definition of layer. In this case, the figure shows an Ethernet packet that is transporting world wide web (HTTP) data.

76. The lowest pair of boxes represents an Ethernet packet (also known as a ***frame***). The left box is the Ethernet header and the right box is the Ethernet payload, which is the entire IP packet. An Ethernet header is shown in the following figure:

Figure 9 — Ethernet header

77. The information is transmitted onto the Ethernet starting with the left edge of the figure. The first information transmitted is the link-layer destination address, followed by the link-layer source address, then finally the type field. The link-layer destination address specifies the specific network device on the LAN to which this packet is to be delivered. The link-layer source address contains the link-layer address of the network device that is sending the packet. Finally, the value of x800 in the type field identifies the payload in this Ethernet packet as an IP packet.

78. The IP part of the packet is shown in the two connected boxes above the Ethernet packet in Figure 7. The format of an Internet Protocol (IP) version 4 packet is shown in the following figure (which is the same as Figure 5, above):

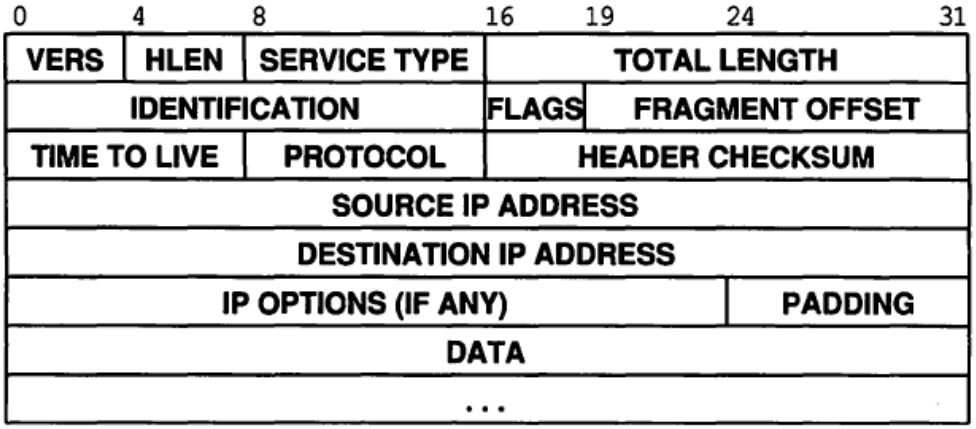


Figure 10 — IP packet format[11]

79. Information is sent on the Ethernet starting in the upper left box of the figure and continuing, row by row, to the lower right. Figure 10 shows the source and destination IP addresses. These are the addresses described above in the definition of layer as network addresses. See below for a fuller description of IP addressing. In this example case, the protocol field will be set to a value of 6 to indicate that the payload of the IP packet (labeled as "data" in the figure) is a TCP packet.

[11] Comer, *supra* note 3.

80. The TCP part of the packet is shown in the two connected boxes above the IP part of the packet in Figure 7. The format of a TCP packet is shown in the following figure:

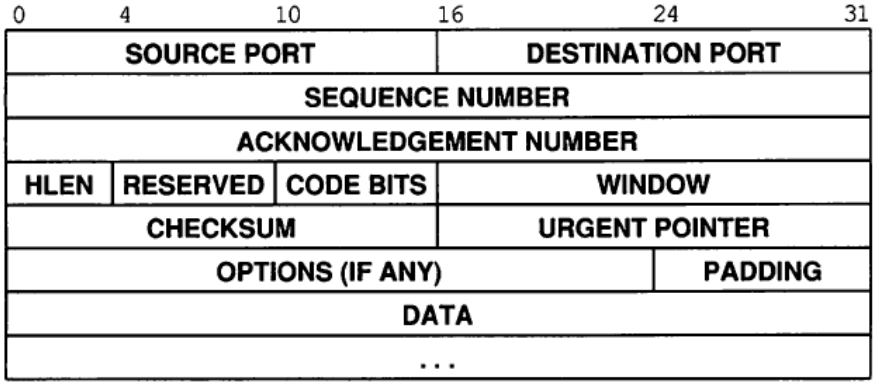


Figure 11 — TCP packet format[12]

81. Information in a TCP packet is sent following the same pattern as with the IP packet. The only field important for this section of this report is the Destination Port field. Since this example packet is carrying world wide web data, the destination port field will be set to a value of 80 or 443. (See below in ¶¶ 110-115 for a fuller description of TCP.) The value 80 in the destination port field indicates that the payload portion (labeled "data" in the figure) is HTTP (world wide web) information and the value 443 indicates that the payload portion (labeled "data" in the figure) is HTTPS, the encrypted version of HTTP.

82. The HTTP part of the packet is shown as the box above the TCP part of the packet in Figure 8. See ¶¶ 117-124 for a fuller description of HTTP.

[12] Comer, *supra* note 3.

9. Switch

83. A ***switch*** is a network node that is connected to two or more network links. A switch receives packets on these network links and forwards each of the packets it receives onto one or more of the other network links based on the destination link-layer address in the link layer of a packet received by the switch. Thus switches are used to forward packets *within* a LAN. Typically there would be an Ethernet switch in some central location on a floor of an office building. Ethernet links would then connect individual desktop computers to the switch.

10. Router

84. A ***router*** is a network node that, like a switch, is connected to two or more network links. A router receives packets on these network links and forwards each of the packets it receives onto one or more of the other network links based on the destination Internet address in the network layer of the packet received by the router. Thus a router is used to forward packets *between* LANs.

11. Mirroring

85. Some switches and some routers have the ability to make copies of some or all of the traffic sent or received on one network link and send that traffic out of a second network link. This is the copying function Dr. Schulzrinne describes in ¶ 58 of his report.

12. Routing

86. ***Routing*** is the process by which a router in a network decides onto which network link the router should forward a packet it has received in order to get the packet closer to the packet's destination, where the destination is represented by the destination Internet address in the received packet. Routers decide where to forward the packets they receive in one of three ways:

a. Routers can be manually configured to determine a forwarding decision.

b. Routers can exchange information with other routers to build a dynamic database of information on which to make forwarding decisions.

c. Routers can be configured to use a combination of the two.

87. See ¶¶ 175-199 for additional discussion on routing in the Internet.

13. Internet Protocol

88. The ***Internet Protocol*** is defined by a set of standards that specify the format of packets in the Internet and how the packets are to be generated by the sender of the packet and processed by the receiver of the packet to enable the transfer of communications between nodes in the Internet. See below for a fuller description of the Internet Protocol.

14. Internet Service Provider (ISP)

89. An ***Internet service provider*** (***ISP***) is a company that provides connectivity between a set of customers and the rest of the Internet. The customers could be individuals using smartphones or computers in their own homes or in enterprises that run their own Internet Protocol-compatible enterprise networks. ISPs range from ones

that service a small part of a small town to ISPs that service customers around the globe. See below for a fuller description of ISPs.

15. Proxy

90. A ***proxy*** is a network node that serves as a forwarding agent for communications between other Internet nodes. In most cases a proxy rewrites the IP packet header information in the communication such that the proxy appears to be the origin or destination of the communication rather than the network node the proxy is serving.

16. Tunnel

91. A ***tunnel*** is a type of virtual network link used to establish what appears to be a direct network link between network nodes by transporting packets flowing between the two nodes within other packets. The transporting packets may traverse multiple network nodes, both switches and routers, on a path between the two tunnel nodes. In many cases the packets being transported over a tunnel are encrypted. An example of an encrypted tunnel is a ***virtual private network*** (***VPN***) that a traveler uses to connect his or her laptop computer in a coffee shop back to his or her employer's enterprise network. Such VPNs are used to protect communications between the laptop and an enterprise network from eavesdropping and to protect communications between enterprise networks.

17. Metadata

92. ***Metadata*** is information about a communication that is not within the communication itself. Examples of metadata include the source and destination IP addresses for a communication, and the time the communication starts and ends.

C. The Key Internet Protocols

93. In the following section, I will describe the key protocols that are used in the Internet today (i.e., the Internet Protocol Suite) and several of the most common ***application protocols*** used on the Internet (i.e., HTTP/HTTPS for web access and IMAP/SMTP for email).

1. The Internet Protocol Suite

94. Kahn and Cerf defined more than just the format of IP packets and how IP packets were created and processed; they defined a suite of protocols. The suite includes the Internet Protocol itself as well as a few "higher-level" protocols that use IP packets for transport and that define ways to support specific types of communication between network nodes. I will describe the Internet Protocol more fully and then mention two of those higher-level protocols below.

a. The Internet Protocol (IP)

95. As mentioned above, there is a defined format for IPv4 packets, which is shown in the following figure which I repeat from above to make it convenient for the reader:

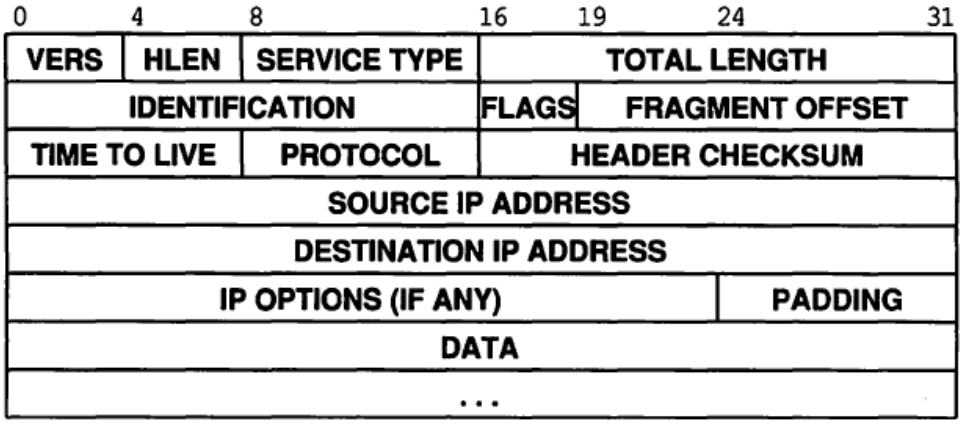


Figure 12 — An IP packet[13]

96. The first part of an IP packet is known as the ***IP header***. The IP header comprises the fields shown in Figure 12 through the optional "padding" field (that is, the first six rows). In addition to the source and destination IP address fields in the IP header that I have already described, there is one other field in the IP header that is relevant to this case. The "protocol" field is used to indicate what higher-level protocol is using the IP packet for transport. When an IP packet is created and sent by a network node, for example by a user's personal computer, the node will put its own IP address into the Source IP Address field and the IP address of the node that it wants to send the packet to into the Destination IP Address field. The computer will also put a value in the protocol field so that the receiving node will know what to do with the packet when it is received.

i. IP addresses

97. An ***IP address*** is a number that is used to identify a particular network device on a network that is using the Internet Protocol for communication. IPv4 addresses are 32-bits long and can identify about 4 billion individual network devices. IPv6 addresses are 128-bits long and can identify trillions of trillions of individual network devices. I will focus on IPv4 in this report, but when I use the term "IP address" it should be taken to mean the type of IP address used in the version of IP in use in the particular situation.

[13] Comer, *supra* note 3.

98. An IPv4 address is represented as a set of 4 numbers separated by periods. For example, the IP address for the web server I run in my house is 173.166.5.74 and, as of this writing, one of the IP addresses of the University of Oxford's website, www.ox.ac.uk, was 129.67.242.155.

ii. Viewing IP header information

99. The IP header information is visible throughout the path a packet takes through the Internet. Except in the cases where the IP addresses are modified in transit, (I will mention some cases of this below), the actual source and destination of each packet in the Internet can be determined by just looking into its IP header.

100. The IP header information must be unencrypted even when the information being transported is encrypted. To transport an email message, for example, the IP header information for the packets that make up the email must be unencrypted so that the routers forwarding the packets know where to send them and so that the receiving node knows what to do with them.

101. Information beyond the IP addresses and protocol can be observed in IP packets by looking further into the packet to get the port numbers and application-specific information. The function of looking into packets to better understand the application-level communications they transport is often referred to as "deep packet inspection (DPI)." I will discuss DPI further below.

iii. Sizes of IP packets

102. IP packets in the Internet are variable in length. They range from a minimum size of 68 bytes long to 1,500 bytes long. The 1,500 byte limit derives from the maximum packet size that is supported on Ethernet, the most common type of local

physical network. A 1,500 byte packet is big enough to transport the body of an email message of up to a thousand characters—about 200 four-letter words (including spaces between each word).

iv. Multiple packets in a communication

103. A particular communication will be broken up into multiple packets by the sending node if the communication cannot fit in a single large (1,500 byte) packet. The packets are reassembled into the communication by the destination node in order to recover the originally transmitted message.

104. The reassembly must be done by the destination node because the Internet does not guarantee that all of the packets that make up a particular communication will be present at any other place along the path from sender to receiver. Two features of the Internet cause this to be the case:

a. The paths that packets take through the Internet can change at any time, even between successive packets in a single communication.

b. The paths packets take are asymmetric, in that packets in a two-way communication traveling in one direction will generally not follow the same path as packets traveling in the opposite direction.

b. Transport Protocols

105. As described above in ¶¶ 50-61, ***transport protocols*** are used to break communications into packets and to provide the desired level of reliability. The two transport protocols I will describe here are the User Datagram Protocol and the Transmission Control Protocol. These are the dominant transport protocols currently in general use on the Internet.

i. The User Datagram Protocol (UDP)

106. The ***User Datagram Protocol*** (***UDP***) provides a way to send packets from one network node to another network node over IP packets. Many applications use UDP for transport, including certain voice and video streaming applications, tunneling protocols, and domain name lookups (see ¶ 184 for a description of how to do domain name lookups).

107. UDP information is carried in the "data" portion of those IP packets that make up a communication using UDP as its transport. UDP has its own header as shown in the figure below:

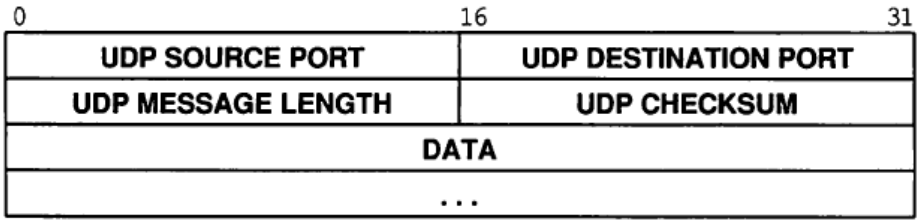


Figure 13 — The UDP header[14]

108. The destination UDP port field is used to specify the application that is running over UDP. Hundreds of applications have been defined to date, many in "open" standards but quite a few in non-public and proprietary ones.

109. UDP port numbers can range from 1 to 65,535. UDP port numbers 1 to 49,151 are "registered" for use by particular applications. Port numbers between 49,152 and 65,535 are "unassigned" and open for use by any application, although the node that receives a UDP packet using an unassigned port number must have been preconfigured to know what to do with a packet with that unassigned destination port number. Note that

[14] Comer, *supra* note 3.

port number assignments are, in a way, advisory. As long as the two ends of a communication agree on which port numbers to use, any port numbers will work, even port numbers that have already been assigned to specific applications. Thus, by changing the port numbers in use, someone can change the apparent application being used. For example, quite a few applications use ports 80 or 443, the ports nominally assigned to the world wide web, because these ports are often passed by firewalls that would block unassigned ports.

ii. The Transmission Control Protocol (TCP)

110. Whereas UDP is used to just deliver packets from one network node to another without worrying about the rate of transmission or even if the packet in fact makes it to the destination network node, ***Transmission Control Protocol*** (***TCP***) is used to provide a *reliable data stream* between network nodes. TCP is used by most major Internet applications including email, the world wide web, file transfer and the control channel of Internet calling protocols such as Skype. TCP has its own header that is present in all packets in a communication making use of TCP:

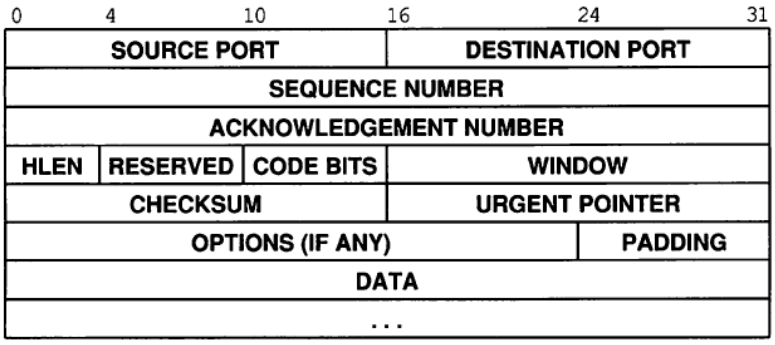


Figure 14 — The TCP header[15]

[15] Comer, *supra* note 3.

111. Two network nodes can use TCP to create and maintain a two-way communications session, to control the rate of packet transmission as appropriate, and to ensure that all of the information in the session will be reliably delivered.

112. TCP can be used to transport a discrete piece of information such as an email message. It can also be used to support continuous streams of information such as a telephone call, although UDP can also be used to transport information streams, including phone calls.

113. Ports in the TCP header are assigned and used in the same way as ports are used in UDP, except that source ports are required. The set of information in the (1) Source and (2) Destination IP addresses fields and the (3) protocol field in the IP header, along with the information in the (4) source and (5) destination port fields in the TCP header, uniquely identifies packets that are part of a particular TCP communication between two network nodes. As explained in ¶ 62, this information is often called a five tuple (or 5-tuple).

114. The sequence number field in the TCP header is used to ensure that all of the packets comprising a communication have been received and that they are in the correct order. This is important because IP networks do not guarantee that packets will not be lost, duplicated or reordered during their travel though the Internet.

115. The Internet protocol suite includes the Internet Protocol itself plus the transport protocols TCP and UDP as well as other signaling protocols and is frequently referred to as "TCP/IP."

2. Application Protocols

116. UDP and TCP are used to transport packets that implement Internet applications. I will discuss a few of the hundreds of applications that have been defined for the Internet.

a. The Hypertext Transfer Protocol (HTTP)

117. The ***Hypertext Transfer Protocol*** (***HTTP***) is used to transport web page content between web servers and web browser software on user computers.

i. HTTP commands

118. HTTP consists of a number of plain text commands sent by a web browser to a web server. The basic HTTP commands are shown in the following figure:

Command	*Description*
GET	Return the contents of the indicated document.
HEAD	Return the header information for the indicated document.
POST	Treat the document as a script and send some data to it.
PUT	Replace the contents of the document with some data.
DELETE	Delete the indicated document.

Figure 15 — HTTP commands[16]

119. The HTTP GET command is used to request that the HTTP server return a file to the user's web browser. The GET command includes the name of the requested file. The POST command is used to upload a file to a web server.

ii. Encrypted HTTP (HTTPS)

120. An encrypted version of HTTP, referred to as ***HTTPS*** (for "HTTP Secure") was introduced in 1994 by Netscape Communications to support electronic commerce over the Internet. The entire HTTP application layer communication is

[16] Lincoln D. Stein, *How to Set Up and Maintain a World Wide Web Site: The Guide for Information Providers* 49 (1995).

encrypted when using HTTPS. The IP packet and TCP header that HTTPS rides on top of are not encrypted, so an observer can determine that an HTTPS session is running between two nodes identified by the IP addresses in the IP header.

121. It is worth noting that not all encryption used on the Internet is "unbreakable." *See* Schulzrinne Decl. ¶ 42. When properly implemented, modern public standards-based encryption itself is generally considered to be unbreakable. But encryption standards are not enough. The software implementing the encryption standard has to be well designed and bug-free, the systems that make use of the encryption must also be well designed and well implemented, and these systems must be properly and carefully operated for the communications to actually be protected.

122. Not all implementations of HTTPS in use on the Internet today are "unbreakable", and the computers making use of HTTPS are all too frequently compromised because of software bugs or user errors. Once a computer is compromised, it is generally easy to compromise any communications as they are being sent or received by that computer. In addition, some developers decide to create their own encryption protocols and algorithms and most of them turn out to be far from unbreakable.[17] In the cases where the NSA determines that the type of encryption protocol or algorithm being used is weak, it would make sense for the NSA to collect encrypted communications from targeted individuals knowing that, with enough effort, for example, with large amounts of computing power the encryption could be broken. The NSA could also be collecting encrypted communications to subject them to quantum cryptanalysis in the

[17] Joseph Cox, *Why You Don't Roll Your Own Crypto*, VICE: Motherboard (Dec. 10, 2015), https://motherboard.vice.com/en_us/article/wnx8nq/why-you-dont-roll-your-own-crypto.

future. Quantum cryptanalysis, which relies on quantum computers, may make it significantly easier to break certain types of encryption in wide use today. It is not publicly known whether the NSA or any other intelligence agency currently has the capacity to conduct quantum cryptanalysis, but encryption standards bodies have been preparing for a number of years for the possibility that intelligence agencies or malicious actors will. The above factors may help to explain the permissive rules (as discussed in ¶¶ 325-327) for the NSA's collection of encrypted communications under Section 702.

iii. HTTPS Handshake

123. Not all of the HTTP information is hidden when using HTTPS. A single physical web server can be used to support many websites. The web server that I run in my house, for example, supports www.sobco.com, www.sobco.org, www.scottbradner.com, and www.kaybradner.com. Because a single web server may be supporting multiple different websites, a web browser must send the domain name of the website to the web server during the setup phase of an HTTPS session so that the web server knows which website the user wants to access and so that the proper security association can be setup. Since the security association has not yet been set up, the domain name must be sent unencrypted. Thus, HTTPS does not protect the confidentiality of the domain name of the website that is being accessed. For example, an observer would be able to determine that a user had requested a web page from https://en.wikipedia.org, but they would not be able to determine from the HTTPS request that the user had requested the specific web page https://en.wikipedia.org/wiki/Addiction.

iv. IP addresses in HTTP packets

124. There are some cases where the IP addresses in HTTP packets do not accurately identify the original sender of a HTTP packet or its ultimate destination. For example, HTTP proxies are sometimes used in enterprise networks, including hotels, and in some Internet service providers to improve the performance of user's web browsers and to control access to improper websites. HTTP packets sent from all web browsers used by everyone behind an HTTP proxy will have the IP address of the HTTP proxy as the IP Source Address in the header. Likewise, the Destination IP Address in all HTTP packets destined to web browsers that are behind an HTTP proxy will have the IP address of the proxy as their Destination IP Address. There are also cases where there are no proxies or NATs (see below in ¶¶ 173-174) where the IP addresses in the packets identify the sender and receiver of a packet.

b. Email

125. As a formal matter, ***electronic mail*** or ***email*** refers to "*a system for sending messages from one individual to another via telecommunications links between computers or terminals using dedicated software*".[18] Email is the third oldest Internet application, behind remote access and file transfer.

[18] *Email*, Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/email.

i. Email Header Information

126. Individual email messages have a format defined in specifications from the IETF[19]. The start of an email message consists of a series of plain text "headers" that include the names and email addresses of the sender and intended receiver(s) of the message, the date the message was sent, a subject for the message, some information about the path the message took through the Internet which generally includes the IP address of the email server that sent the message, and some information about the format of the body of the message, i.e. the part of the message following the header lines. Very often, an email message will not fit in a single packet. In such cases the header lines will start in the first packet of the communication, but sometimes the header lines will extend into the second packet.

127. An example of some of the entries in an email header are shown in the following figure:

```
From: "Scott O. Bradner" <sob@sobco.com>
Content-Type: text/plain;
        charset=us-ascii
Content-Transfer-Encoding: 7bit
Mime-Version: 1.0 (Mac OS X Mail 11.3 \(3445.6.18\))
Subject: need to reschedule Taveras appt
X-Universally-Unique-Identifier: 78BC10A7-0A77-4C96-96D0-9C394F696E8E
Message-Id: <40D15B68-D405-46CC-A511-24F809988261@sobco.com>
Date: Thu, 5 Apr 2018 09:52:37 -0400
To: "Cheryl F. Chapman" <cfc@sobco.com>
```

Figure 16 — Sample email header

128. The above is the header portion of an email message from me to my wife. The "From:" header line provides my name and email address as the sender of the email

[19] See, e.g., *Internet Message Format*, Qualcomm Inc., Network Working Group (October 2008), https://www.ietf.org/rfc/rfc5322.txt.

message. The "To:" line shows my wife's name and email address as the destination of the message. The "Subject:" line shows what I said was the subject of the message. The "Date:" line shows the time I sent the message. Finally, the "Message-Id:" line is a unique identifier for this particular message. The body of the message that follows the header lines could be plain text, one or more photos, one or more pieces of video or music, a spreadsheet, a Microsoft Word document, a pdf, or any one of dozens of other things. In addition, the body of an email message may or may not be encrypted.

ii. Email Servers

129. As a general rule, email messages do not go directly from a sender to a receiver. Instead, there could be an email server at the sending end, and there is almost always an email server on the receiving end. Email servers maintain databases of sent and received email messages for each of their users.

130. Email users access their email servers by using a web browser or by using a piece of software called a "mail user agent" on their own computer. With the web browser or mail user agent, an email user can create and send email messages and also read any email he or she might have received.

131. Many large commercial email services, such as Hotmail and Gmail, are accessed via web browsers. Some large commercial email services, for example Microsoft Exchange, are accessible via web browsers but are also accessible via their own special mail user agents. In addition, some computers come with their own generalized mail user agents that can connect to multiple commercial email services. One example of the latter is the Mail program that comes with Apple computers. This is the mail user agent that I use. I use the Apple Mail application to connect to Harvard's Microsoft Exchange server, Google Gmail and to the email server that I run in my house.

132. Mail user agents generally download all new email messages to the user's computer whenever the mail user agent is started. Thus, when an email user turns on their laptop after a few days "off line" a burst of email messages can be transferred to the laptop. Such bursts will often be done over a single communications session between the email server and the mail user agent, resulting in multiple individual email messages in the same communication. Some web mail implementations do the same type of burst fetch of unread email. This behavior may be an example of what the NSA has called a multi-communication transaction (MCT) since the NSA says that an MCT can consist of multiple email messages.[20] (See above at ¶¶ 66-68 and below at ¶¶ 316-320.)

133. There are a number of IETF protocols that define the communications between email servers and between email servers and mail user agents. In addition, there are some proprietary protocols. I will discuss the two most common, standards-based protocols:

a. ***Simple Mail Transfer Protocol*** (***SMTP***): used between email servers and between email servers and some mail user agents

b. ***Internet Message Access Protocol*** (***IMAP***): used between most mail user agents and email servers.

iii. Simple Mail Transfer Protocol (SMTP)

134. The Simple Mail Transfer Protocol (SMTP) is used to transport email messages between email servers and, less frequently, between mail user agents and email servers. The SMTP protocol defines a ***handshake*** that is used to start up a session to transfer an email message. A sample of an SMTP handshake used when a user is sending

[20] Appendix E at 15-16 n.17 (FISC Opinion (Apr. 26, 2017)).

an email message is shown in the following figure, where "S" identifies text sent by the email server and "C" identifies text sent by the email client:

```
S: 220 Beta.GOV Simple Mail Transfer Service Ready
C: HELO Alpha.EDU
S: 250 Beta.GOV

C: MAIL FROM:<Smith@Alpha.EDU>
S: 250 OK

C: RCPT TO:<Jones@Beta.GOV>
S: 250 OK

C: RCPT TO:<Green@Beta.GOV>
S: 550 No such user here

C: RCPT TO:<Brown@Beta.GOV>
S: 250 OK

C: DATA
S: 354 Start mail input; end with <CR><LF>.<CR><LF>
C: ...sends body of mail message...
C: ...continues for as many lines as message contains
C: <CR><LF>.<CR><LF>
S: 250 OK

C: QUIT
S: 221 Beta.GOV Service closing transmission channel
```

Figure 17 — SMTP startup handshake[21]

135. The SMTP handshake includes the message sender's email address (Smith@Alpha.EDU) and the email address of the intended recipients of the message (Jones@Beta.GOV, Green@Beta.GOV and Brown@Beta.GOV). Even if parts of the body of an email message are encrypted, the SMTP handshake is not, although the entire SMTP exchange could take place within an encrypted connection, in which case the

[21] Comer, *supra* note 3.

SMTP handshake would be encrypted, and any encrypted parts of the email message would be doubly encrypted.

(1) SMTP Metadata

136. The sender's and receiver's email addresses as well as the date and time that the mail was sent and the IP addresses of email servers would all be considered email metadata. This metadata is included in the SMTP startup handshake as well as in the email headers.

(2) IP addresses in email packets

137. The IP addresses in the packets exchanged between email servers identify the email servers but often have no relationship to the actual sender or receiver of an email message. Some mail user agents are configured to use SMTP to send email messages directly to the email server associated with the intended recipient. In such cases the source IP addresses in packets sent to the email server will identify the computer that is running the mail user agent.

iv. Internet Message Access Protocol (IMAP)

138. IMAP defines the formats and meanings of the messages exchanged between a mail user agent and an email server. In general, these messages are used to maintain a copy of the email user's portion of the email server on the user's own computer.

139. As mentioned above in ¶ 132, when a mail user agent connects to an email server using IMAP, all new messages will be downloaded to the user's computer in a batch.

140. In my own case, the mail user agents on my laptops, desktops and smartphone are configured to use IMAP to connect to the email server I run in my house

when sending email. The IP addresses in the packets my email server sends will be the IP address of that server, no matter where in the world I might be. Similarly, packets comprising an email message sent by a Gmail user will include the IP address of the Gmail server in their source address field no matter where the Gmail user is actually located.

c. Telephone Calls

141. While it's not part of this case, a number of NSA documents say that the NSA collects telephone calls and that telephone numbers are one type of selector that is used to target Internet transactions, under the upstream collection program. Since almost all international telephone calls are currently transported over the Internet using the IETF-developed Session Initiation Protocol (SIP), it is easy to include them in the upstream program. SIP has HTTP-like headers that are used to specify the source and destination telephone numbers and the IP addresses between which the audio portion of the phone call will flow.

3. Plain Text in Application Protocol Headers

142. Many Internet applications, including the applications mentioned above, include "plain text" (i.e., not encrypted and not otherwise encoded) fields in their headers. Such fields can be searched for specific strings such as a name or email address or other string that might indicate that a packet is part of a communication that is of interest, even if portions of the underlying communication are encrypted. These text fields will sometimes be entirely in the first packet of a flow of packets that makes up a communication but often do extend into successive packets.

4. Number of Packets in a Communication

143. As described above in ¶ 49, a particular communication between nodes over the Internet is broken up into packets for transmission. The number of packets in any one communication varies greatly. The sample email message between me and my wife shown above was short enough to be contained within a single packet (although the SMTP handshake that would've preceded the email when sent between email servers would have required an exchange of multiple separate packets), but I sent an email message to a colleague recently that contained two image files. The message was 2.7 million bytes (MB) long so it took at least 1,860 packets to transport that message. I frequently send email messages that are 10 MB or more. It takes thousands of packets to transport each of those messages.

144. I ran a command on the router that interfaces the network in my house to my Internet service provider that asked for statistics on the number of packets in a flow. The results of that command are shown in the following figure:

Protocol	Total Flows	Flows /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active(Sec) /Flow	Idle(Sec) /Flow
TCP-Telnet	14222087	3.3	1	43	4.1	1.0	15.5
TCP-FTP	113213	0.0	2	60	0.0	1.9	14.4
TCP-FTPD	13567	0.0	1	40	0.0	0.0	15.4
TCP-WWW	2967948	0.6	81	846	56.1	24.5	8.2
TCP-SMTP	3454819	0.8	7	261	5.9	2.0	5.7
TCP-X	328461	0.0	1	40	0.0	0.0	15.4
TCP-BGP	14779	0.0	1	40	0.0	0.0	15.4
TCP-NNTP	8667	0.0	1	40	0.0	0.0	15.4
TCP-Frag	174	0.0	1	460	0.0	0.1	15.4
TCP-other	50802851	11.8	20	432	245.9	4.5	9.1
UDP-DNS	324539	0.0	2	63	0.1	0.7	15.4
UDP-NTP	597821	0.1	1	76	0.1	0.0	15.4
UDP-TFTP	28463	0.0	1	42	0.0	0.0	15.4
UDP-Frag	36396	0.0	1	540	0.0	0.0	15.5
UDP-other	68219772	15.8	1	224	17.6	0.3	15.4
ICMP	1701074	0.3	5	63	2.2	9.4	15.4
IPv6INIP	14	0.0	1	80	0.0	0.0	15.4
GRE	57855	0.0	2111	209	28.4	29.1	15.3
IP-other	451	0.0	1	53	0.0	0.0	15.5
Total:	142892951	33.2	10	459	360.9	2.5	12.8

Figure 18 — Average flow lengths in my home router

145. The printout shows the statistics since the router was last rebooted a few years ago. The results show that the average length of the email messages that I sent or received over the past few years was 7 packets (TCP-SMTP) and the average length of my web sessions over the same time period was 81 packets (TCP-WWW).

146. I do not think that these statistics are necessarily representative of general Internet traffic, but they do show that much Internet traffic consists of communications comprising multiple packets.

D. Other Features of the Internet and its Architecture Relevant to this Case

147. In the following section, I will describe other features of the Internet and its architecture that are relevant to this case, including the general structure of the Internet, the role of Internet Service Providers, the way in which networks comprising the Internet connect to one another, the meaning of the "Internet backbone," the undersea fiber optic cables that connect the U.S. to the rest of the world, and the way that packets are routed on the Internet.

1. Internet Architecture

148. There is no fixed architecture to the Internet. Each customer and service provider is free to design and operate their network or networks in any way they want as long as they are able to transport IP packets along a path from the packet source to the packet destination. Each network operator is also free to interconnect their networks with networks run by other network operators in any way that the two operators agree to, as long as they can properly transport IP packets between the networks.

149. The result is that the Internet structure appears almost random as shown in the following figure from the Opte Internet mapping project:

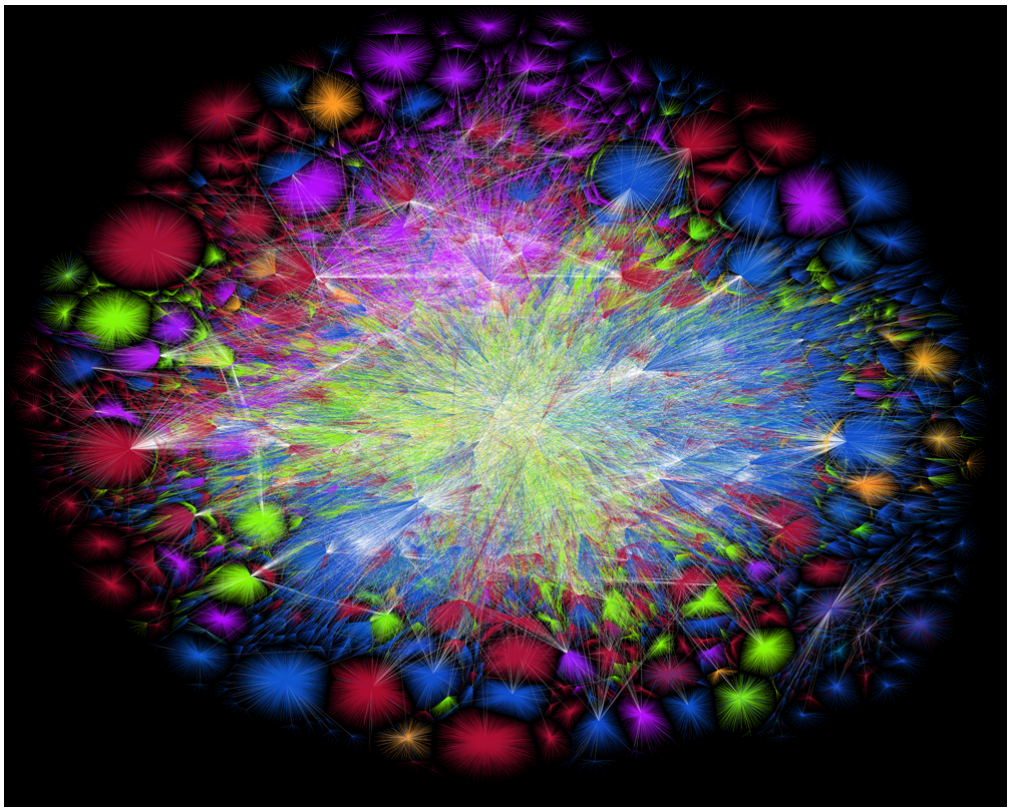


Figure 19 — The Internet[22]

2. Internet Backbone

150. One of the terms used in this case is "the Internet backbone." Once upon a time, between 1983 and about 1990, it was easy to define the Internet backbone in the U.S. In 1983 it was the ARPANET. The ARPANET was the only nation-wide network that was being used to interconnect other networks, so it was "the Internet backbone." By 1990, the ARPANET had been joined by the NSFNet and the first few commercial ISPs. But there were very few of these ISPs that were nation-wide, so it was reasonable

[22] The Internet 2015, The Opte Project (July 11, 2015), http://www.opte.org/the-internet.

to say that the Internet backbone consisted of the long distance connections in the ARPANET, NSFNet and those ISPs that provided nation-wide service.

151. Since then the growth of ISPs of all sizes and the end of the ARPANET and NSFNet have painted an increasingly more complex picture, to the point that today it is not possible to isolate a single backbone for the U.S. Internet, much less the global Internet. The term "Internet backbone" is one that shows up in the popular press from time to time, but my experience is that experts in the field tend not to use that term. Occasionally, I have seen reference to the "Internet backbones" (plural), referring to the largest ISPs, but more often I've seen references to "ISP backbones", not to an Internet backbone. In an ISP, the backbone is the set of high-speed lines that interconnect routers in different parts of the ISP's geographic footprint.

152. The NSA has provided one interrogatory response and two admissions in regard to their use of the term "Internet backbone":

a. *NSA Defendants respond that to their understanding the Internet backbone is no longer well defined due to the growth of direct peering arrangements, but may be understood as the principal high-speed, ultra-high bandwidth data-transmission lines between the large, strategically interconnected computer networks and core routers that exchange Internet traffic domestically with smaller regional networks, and internationally via terrestrial or undersea circuits.*[23]

b. *NSA Defendants respond that yes, the Internet backbone includes but is not limited to international submarine telecommunications cables that carry Internet communications.*[24]

[23] Appendix D at 18 (NSA Response to Plaintiff's Interrogatory No. 12 (Dec. 22, 2017)).

[24] Appendix H at 6 (NSA Response to Plaintiff's Request for Admission No. 3 (Jan. 8, 2018)).

c. *NSA Defendants respond that yes, the Internet backbone includes but is not limited to high-capacity terrestrial telecommunications cables that carry Internet communications within the United States.*[25]

153. In summary, the government's definition of the Internet backbone includes (1) the high-speed circuits (network links) and routers that are used to interconnect ISPs, (2) the circuits in the undersea cables that connect the U.S. with other countries, and (3) the high speed terrestrial network links (circuits) within the U.S and between the U.S. and other countries. The latter two may be network links between ISPs or within an ISP. I will adopt the government's definition for this report.

154. As stated above in ¶ 70, the Internet is a network of networks. Some of these networks are very small, like the one in my house, and some are very large such as AT&T's IP network, which spans the globe. These networks include customer networks and service provider networks. Each of these millions of networks is under its own management—there is no central manager for the Internet.

3. Internet Service Providers (ISPs)

155. The purpose of service provider networks, known as Internet service providers (ISPs), is to provide "the Internet" to the customer networks that purchase Internet connectivity from the ISP. Each ISP itself consists of multiple interconnected networks. ISPs connect to their customer networks through a link between an IP router in the ISP network and a switch or router in the customer network.

[25] Id. (NSA Response to Plaintiff's Request for Admission No. 4 (Jan. 8, 2018)).

156. According to broadbandnow.com, an Internet site providing information to people looking for ISPs in their area, there are over 2,600 ISPs in the U.S.[26] The ISPs range in size from the big carriers (such as AT&T Wireless and Verizon Wireless, which offer services in all 50 states plus some territories), to the large cable TV companies (which offer ISP service in as many as 40 states), to very small ISPs (such as Surge Communications, which offers Internet services in two just zip codes).

157. For example, Comcast offers its Xfinity Internet service in parts of 40 states. The Xfinity coverage is shown in the following figure:

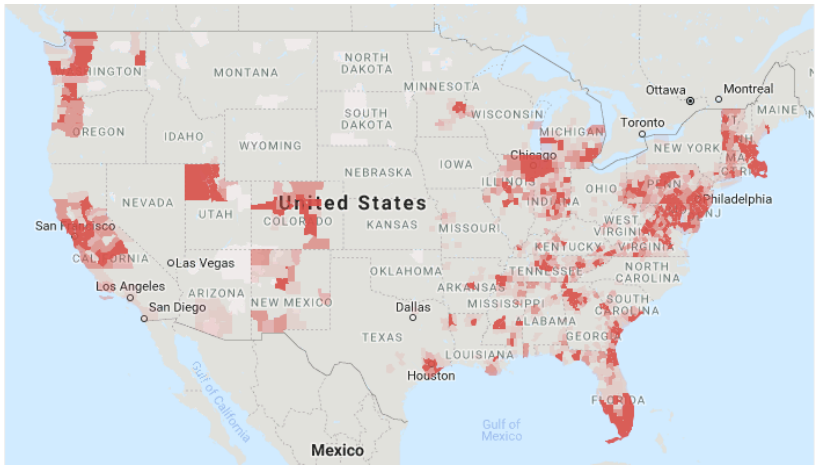


Figure 20 — Xfinity coverage[27]

[26] *Internet Providers in the U.S.*, Broadband Now, https://broadbandnow.com/All-Providers.

[27] *Xfinity From Comcast Availability Map*, Broadband Now, https://broadbandnow.com/XFINITY (last updated Dec. 1, 2018).

158. A small ISP such as Orca Communications has a still smaller service area, in this case a small part of the southwest coast of Oregon:

Figure 21 — Orca Communications service area[28]

a. Address assignments for ISPs

159. Larger ISPs are assigned ranges of IP addresses by one of five Regional Internet Registries (RIRs), each of which is responsible for a part of the globe. The ISPs use the assigned addresses for their own networks, and they subassign some of the addresses to their customers for use in the customer's own networks.

160. Over the last few years a commercial market has developed for the right to use blocks of IP addresses.[29] Individual ISPs or companies can purchase the right to use a block of addresses from someone who currently has that right and then register the

[28] *Orca Communications Availability Map*, Broadband Now, https://broadbandnow.com/ORCA-Communications (last updated Dec. 11, 2018).

[29] Paul McNamara, *MIT Selling 8 Million Coveted IPv4 Addresses; Amazon a Buyer*, Network World (Apr. 21, 2017), https://www.networkworld.com/article/3191503/internet/mit-selling-8-million-coveted-ipv4-addresses-amazon-a-buyer.html.

block with one of the RIRs. The addresses do not have to be used in the same geographic area as they were being used before they were purchased.

4. ISP Interconnection

161. Because no one ISP connects to all of the customer networks that make up the customer network part of the Internet, ISPs must interconnect with other ISPs to get connectivity to the customer networks they do not directly serve. Each ISP decides on its own how to interconnect with other ISPs to get full Internet connectivity.

162. As a general rule, similarly sized ISPs interconnect with each other with little or no fees exchanged for the interconnection. This type of interconnection is known as ***peering***. Small ISPs must become the customers of larger ISPs in order to be able to interconnect with the larger ISP. The smaller ISP must pay for the interconnection, as any customer must. In general, the interconnections any one ISP maintains are considered proprietary information.

163. ISPs interconnect with other ISPs, either as customers or as peers, through private interconnections and through Internet exchange points.

164. Private interconnections are direct links from a node in one ISP's network to a node in another ISP's network. When large ISPs peer with other large ISPs, they do so at multiple geographically dispersed locations to ensure that traffic between the ISPs can be as distributed as the traffic sources or destinations are, and to ensure reliability through redundancy. For example, AT&T's peering policy requires a minimum of 6 peering points.[30] Large ISPs that peer with multiple other large ISPs are sometimes referred to as ***Tier 1 ISPs***. The ISPs generally considered to be Tier 1 ISPs in the U.S.

[30] *AT&T Global IP Network Peering Policy*, AT&T Business, https://www.corp.att.com/peering.

include AT&T, Verizon, Sprint, Century Link and Level 3. Tier 1 ISPs in Europe include FranceTelecom, Telefonica and Deutsche Telecom.[31]

165. An ***Internet exchange point*** (known as an ***IX*** or an ***IXP***) is a node, usually an Ethernet switch, which has links to nodes in multiple ISPs. Each ISP connected to the exchange point can use the exchange point to interconnect with any other ISP connected to the same exchange point subject to bilateral agreements between the ISPs. The operator of the exchange point need not be a party to any agreement between ISPs to exchange traffic.

166. A single ISP, particularly the large ones, can be connected to multiple Internet exchange points, sometimes in multiple countries or even continents[32]

5. Customer Networks

167. Customer networks in the Internet include the small ones such as the one in my house, as well as much larger networks such as the Harvard University's network, Google's internal network and the network at the U.S. Department of Agriculture. Most customer networks themselves consist of many interconnected individual networks.

168. The individual networks that make up a customer network might consist of one or more links, such as physical Ethernet links, interconnected with one or more switches or it might just consist of a single WiFi (wireless) network. The different individual networks that make up a customer network are interconnected with IP routers. For example, I have a physical Ethernet network with multiple Ethernet switches and two

[31] *Who Are the Tier 1 ISPS?*, Dr. Peering International, http://drpeering.net/FAQ/Who-are-the-Tier-1-ISPs.php.

[32] For example, see the list of the exchange points the Australian ISP Telstra peers at: Telstra (International), PeeringDB, https://www.peeringdb.com/net/1459.

WiFi networks in my house. These networks are connected together through an IP router, which I manage.

169. Harvard's network consists of a few hundred separate physical Ethernet networks, each consisting of Ethernet links to individual computers and Ethernet switches to interconnect the Ethernet links. The Harvard network also includes a few dozen WiFi networks. The individual Ethernet networks and the individual WiFi networks are interconnected with many IP routers. Google's internal network spans the globe and consists of an unknown (to me) number of individual networks interconnected through routers.

170. Each individual network in a customer network is assigned its own range of IP addresses to be used by the nodes, such as users' computers attached to that network. Generally, the overall customer network is assigned one or more larger blocks of IP addresses and the individual networks are assigned sub parts of the larger blocks.

a. Address assignments for customer networks

171. Most residential or small enterprise customer networks do not have fixed IP addresses on the Internet. Instead they use one or more IP addresses assigned by their ISP that may change from time to time. Larger enterprises can obtain fixed address assignments directly or, for an extra fee, from their ISPs. With some exceptions, networks that are not assigned fixed IP addresses cannot support Internet services such as email servers or web servers.

6. Customer Network Interconnection

172. As a general rule with some exceptions, customer networks do not interconnect directly with other customer networks. Instead customer networks connect to ISP networks to get Internet connectivity, including connectivity to other customer

networks. Customers expect to get access to the whole Internet when they purchase Internet service from an ISP.

7. Network Address Translators (NATs)

173. ***Network address translators*** (***NATs***) are network nodes that sit on the edge of an individual network, a group of networks or even a whole customer network. Their purpose is to translate the IP addresses in the header of an IP packet and the port numbers in the TCP or UDP header such that all of the network nodes on the network appear to have the same IP address. By sharing IP addresses in this way, NATs reduce the demand for the somewhat limited number of IPv4 addresses, and they can hide the internal structure of a network from observers outside of the network, which is seen as a security advantage.

174. But an effect of NATs is that individual computers whose packets pass through a NAT do not have separate IP addresses; they all have the same IP address that was assigned to the NAT, so the communications cannot be distinguished merely by looking at the IP addresses in the packets that make up the conversation.

E. Routing in the Internet

175. Networks comprise one or more network links interconnected with switches. Networks are connected to other networks through routers.

176. As described above in ¶¶ 71, 84, the network nodes that are used to connect one network to another in the Internet are called routers. This is the case within a customer network, within an ISP network, between a customer network and an ISP network, and between ISPs.

177. For routers to know where to forward packets, they must understand the topology of a relevant part of the network. They gain this understanding by exchanging information with other routers within the name network. The same is true for the routers used to interconnect ISPs—they exchange information so that they can understand the Internet topology well enough to know where to forward packets they receive.

178. Routing protocols define the mechanisms the IP routers use to exchange this topology information. IP routers within a customer network or within an ISP network use a type of routing protocol designed to be used where all the IP routers are run by the same organization such that information from them can be trusted. Such a routing protocol is called an ***Interior Gateway Protocol*** (***IGP***). The two most common IGPs are Open Shortest Path First Routing Protocol (OSPF) and Intermediate System to Intermediate System Routing Protocol (IS-IS).

179. The routing protocol used between ISP networks and other ISP networks or between ISP networks and some of their larger customers is called an ***Exterior Gateway Protocol*** (***EGP***). The only EGP in current use in the Internet is Border Gateway Protocol version 4 (BGP4). ISPs do not generally run a routing protocol between themselves and their customer networks unless the customer has connected their network to multiple ISPs. In such cases, BGP4 is used.

180. Unlike with IGP routing protocols, EGPs operate in an environment where the different routers are operated by different organizations, and an ISP needs to be able to define the level of trust it wants to have in particular information from particular other ISPs or from their customers. Thus, BGP4 has an extensive set of mechanisms to let the operators of routers configure just what information they want to accept from other

routers and what information they want to provide to other routers. The configuration of these mechanisms in a router is done by the router operator. There are no general rules as to what the configuration should be.

1. Autonomous System (AS)

181. A set of routers under common administrative control, such as the routers within a customer network or within an ISP, are assigned an ***Autonomous System number*** for identification. For example, many of the routers at Harvard are assigned AS 11. AS numbers are used by routing protocols as a way to refer to a part of a network or to a whole network such as an ISP.

2. Routing an IP Packet

182. I will now walk through the process by which an IP packet is transported across the Internet, taking as an example my connecting to a web server.

183. In the first step, I type a URL which specifies a particular resource, such as a picture, on a specific website into the window at the top of my web browser, or I click on a link that specifies the same resource. I will use the website for the University of Oxford in England (www.ox.ac.uk) as an example website.

184. For my computer to be able to send a packet containing an HTTP request to www.ox.ac.uk, the computer needs to find out what IP address has been assigned to www.ox.ac.uk. This address is needed so it can be put in the destination IP address field of the packets my computer wants to send to www.ox.ac.uk. Computers use the ***Domain Name System*** (***DNS***) to convert the domain name in the URL into an IP address. At the time of this writing, one of the IP addresses for www.ox.ac.uk was 129.67.242.154.

185. My computer then creates a packet containing the HTTP command my browser wants to execute, likely a GET command, and puts the IP address of www.ox.ac.uk in the destination IP address field in the packet. My computer also puts its own IP address into the source IP address field in the packet. Then, using link-layer addressing, my computer sends the packet to my local router.

186. My local router then looks up the destination IP address in the router's ***routing database*** (also called a ***routing table***). This is the database maintained by the routing protocol. Using the information in the routing database, my local router determines which router the packet needs to go to next on its way toward the web server.

187. In general, my local router's routing table will not have an entry for the specific range of IP addresses that includes the IP address for www.ox.ac.uk. This is because there are many millions of such address ranges and my local router does not have the memory space or processing power to keep track of them all. Instead my local router, after determining that it does not have an appropriate entry in its routing table, uses a ***default route*** configured into the router to identify the ***next-hop router***. Using link-layer addressing, my local router then forwards the packet to that "next-hop router".

188. As a general rule, unless specifically configured otherwise, a router will try to find the "best" next-hop router where the determination of "best" is based on the "cost" of sending a packet through that next-hop router to the destination.

189. In an IGP, cost is generally determined by the number of routers the packet will need to traverse within a customer or ISP network in combination with the speed of the links between the routers.

190. In an EGP, cost is generally based on the number of ISPs (identified by their AS numbers) that the packet will need to traverse across the Internet to reach a destination. I say "generally" because the operator of the router can modify the router's configuration so as to determine the criteria. ISP operators configure the routers they use to connect to other ISPs to filter the routing information they accept from the other ISPs and the routing information they send to those ISPs. ISP operators do this to reject known bad routing information, to prefer next-hop routers in ISPs they have peering contracts with, to prefer some next-hop routers for load balancing reasons, and for a number of other operational reasons. (Dr. Schulzrinne's declaration states that a router may route packets to avoid congested connections. No IGP or EGP routing protocols currently in use on the Internet take "congestion" into account in routing packets. *See* Schulzrinne Decl. ¶ 40. That said, some ISPs do manually reroute traffic to avoid overloaded links.)

191. The next-hop router performs the same type of address lookup process to determine the router that is the next-hop from its point of view.

192. This process continues, hop by hop, until a router recognizes that the address is one on a link directly connected to that router. When a router recognizes this, it uses link-layer addressing to forward the packet to the web server.

193. The decision as to the next-hop router can change at any time based on the most up-to-date information in the routing table in the router, so the next packet in my message to www.ox.ac.uk could be sent to a different next-hop router. I will discuss routing table volatility in the next section.

3. Volatility of Routing Information

194. The Internet today consists of millions of network links and millions of nodes, including switches and IP routers. Changes in state may not occur all that often in each one of these routers and links, but with millions of routers and links, each of which are subject to failures, the overall rate of state change can be significant. Each of these state changes can result in a routing update propagated throughout the Internet. Each of the routers receiving the update updates its own routing, which may produce a change in the next hop a particular packet may be forwarded to and, thus, the links a packet will traverse. Changes in router or link state can result from many things, including local power outages, equipment failures, management induced changes (e.g., turning off a link for debugging or, as mentioned above, rerouting traffic to avoid overloaded links) and physical damage to wires.

195. The following figure shows the rate of changes seen at a particular exchange point in September 2013:

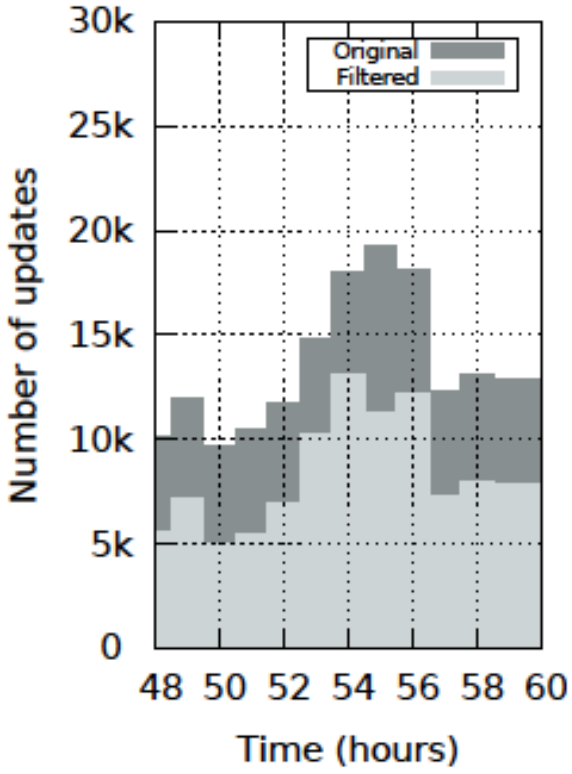


Figure 22 — BGP updates at an Equinix exchange point in September 2013[33]

196. The figure shows the number of updates seen per hour over a 12-hour period starting September 19, 2013 at midnight GMT. The lighter grey area shows the number of unique updates per hour. For example, during the hour between 1 AM and 2 AM there were about 7,000 updates—a rate of almost two updates per second. Since BGP routing updates are propagated throughout the Internet, the same rate of updates will be seen by BGP routers all over the Internet.

[33] Appendix I at 4 (David Hauweele et al., *What Do Parrots and BGP Routers Have in Common?*, Computer Comm. Rev. (July 2016), https://ccronline.sigcomm.org/wp-content/uploads/2016/07/sigcomm-ccr-paper26.pdf)).

4. Asymmetric Data Paths

197. The packets the web server sends back to my web browser in response to my hypothetical request follow the same process. Each router along the path makes its own determination of the next-hop router. Because of this there is no guarantee that the return packets will follow the same path that the request packets took.

198. I mentioned above in ¶ 164 that when large ISPs interconnect with other large ISPs, they generally do so at multiple geographically distinct places. As a general rule, ISPs configure their routers with special rules for the forwarding of packets that are destined to pass through another ISP. The ISPs generally configure the routers to send such packets to the other ISP through the closest interconnect even if that would not otherwise be the "best" path. Since both ISPs do the same, the paths packets take going in one direction can be very different than the paths packets take coming back. This configuration results in asymmetric paths for packets going in opposite directions between two network nodes. This type of routing is known as "nearest exit routing" or "hot-potato routing"—i.e., the ISP passes the packets off to another ISP as fast as it can.

199. Dr. Schulzrinne's description of routing in ¶¶ 41, 89 is incomplete in his failure to mention the asymmetric routing of communications. He states in ¶ 41, for example, that "*packets traveling between two points on the Internet generally follow the same path for long distances*". This is generally true for packets traveling in a particular direction, unless the ISP decides to change the path as I mention above in ¶ 190. But packets going in one direction between two points commonly take a very different path than packets going in the other direction between those same two points, due to asymmetric routing. You can think of the ISP forwarding rules that result in asymmetric routing as similar to one-way streets, causing the route you take from home to the

restaurant, for example, to be different from the route you take from the restaurant back home.

F. International Connections

200. The heavily redundant connections between ISPs are reduced somewhat when it comes to intercontinental connections due to the relatively few undersea physical connections. Note that I'm referring to all of the cables connecting the U.S. to other countries as ***undersea*** even though one of them runs under Lake Ontario and would be more properly called an underlake cable. In addition to these undersea fiber cables, the U.S. is interconnected with Canada and Mexico with many ***terrestrial*** fiber cables. There are also some satellite-based interconnections, far fewer than there used to be before so many fiber cables were installed. Satellite-based connections are of far lower capacity than fiber-based ones and, because of the extra distance the signal has to travel up to the satellite and back, have added delays. Thus, satellite-based international communications are generally limited to islands that have not yet been connected with fiber cables, places far away from civilization and expensive satellite telephones. Since the vast majority of international Internet communications is transported over fiber, I will concentrate on that transport mode.

201. There are over 50 undersea fiber optic cables that connect the U.S. to other countries.[34] In addition, there are a number of fiber optic cables connecting the U.S. to Canada and to Mexico. The following figures are from TeleGeography, a well-regarded source of information about the telecommunications industry including, in particular,

[34] Appendix J (Report on International Submarine Cables Landing in the US, based on information compiled from Telegeography (Jan. 2018)).

maps of undersea cables. The first figure shows the undersea fiber cables connecting the U.S. to other countries as of early 2018:

Figure 23 — Undersea fiber cables[35]

202. The following figure shows the trans-Atlantic cables:

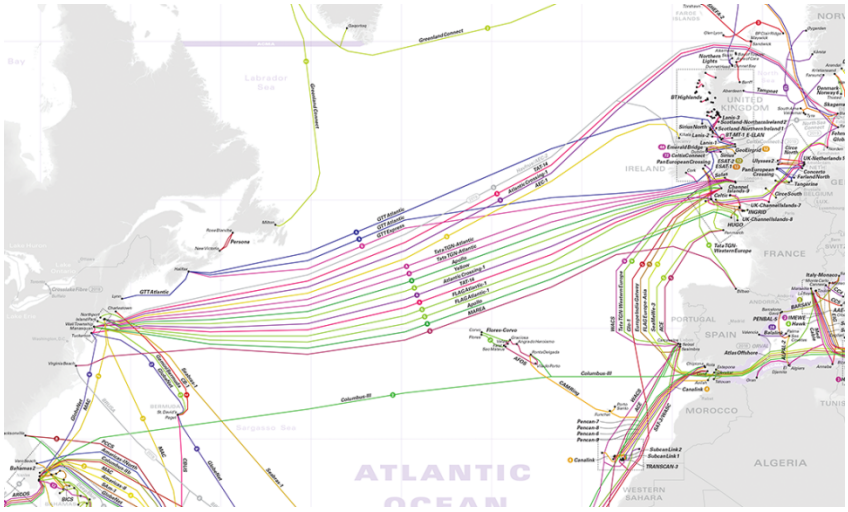


Figure 24 — Trans-Atlantic undersea fiber cables[36]

[35] *Submarine Cable Map 2018*, TeleGeography, https://www.submarinecablemap.com/#/submarine-cable/tat-14.

[36] Id.

203. The following figure shows the trans-Pacific cables:

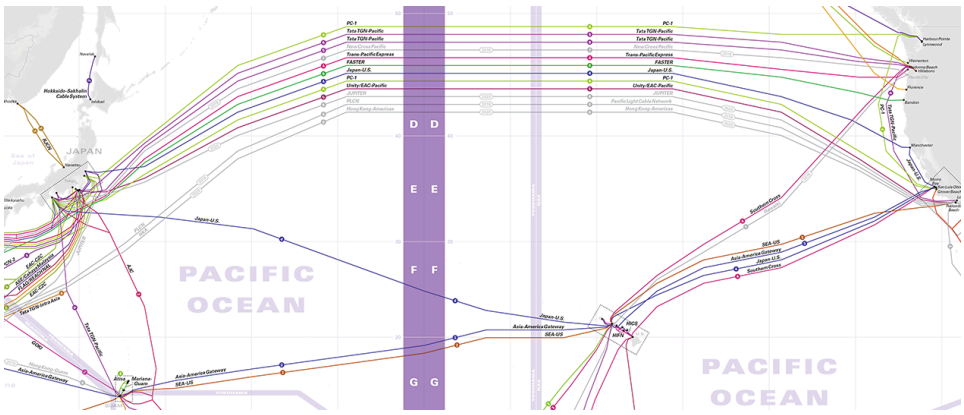
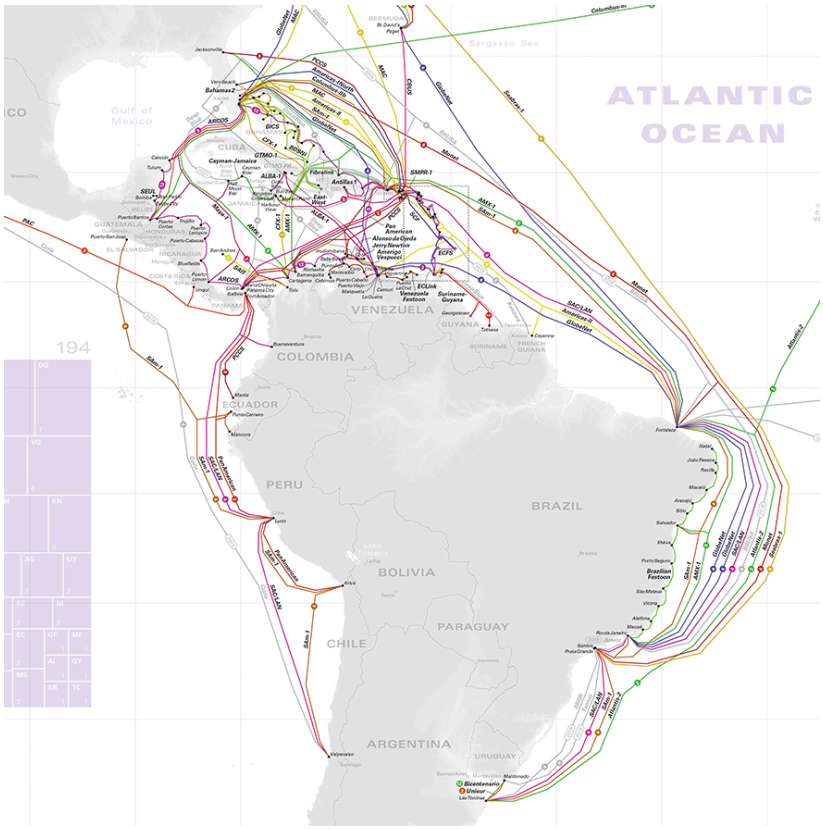


Figure 25 — Trans-Pacific undersea fiber cables[37]

204. The following figure shows the undersea cables servicing South America and the Caribbean:



[37] Id.

Figure 26 — Undersea cables between South America, the Caribbean and Europe[38]

205. The following figure shows terrestrial cables between the U.S. and Canada and between the U.S. and Mexico.

Figure 27 — Terrestrial cables between the U.S. and Canada and between the U.S. and Mexico[39]

1. Details of Undersea Fiber-Optic Cables

206. Each of the undersea cables contains multiple fiber pairs. One fiber in each pair is used to send traffic in one direction, and the second fiber in a pair is used to send traffic in the other direction. Each fiber can support multiple different simultaneous circuits, one on each of a number of colors of light, referred to as ***lambdas***. For example, one of the older transatlantic cables, the TAT-14 cable, has 4 pairs of fibers, each fiber of which supports 40 lambdas, for a total of 160 lambdas in each direction.[40] Each lambda

[38] Id.

[39] *ITU Interactive Transmission Map*, Int'l Tele-Comms Union, https://www.itu.int/itu-d/tnd-map-public (last updated Nov. 2018).

[40] *About the TAT-14 Cable Network*, TAT-14 Cable System, https://www.tat-14.com/tat14.

can support up to 40 gigabits per second (Gbps).[41] The full TAT-14 cables currently support 3.15 terabits per second (Tbps) each. A map of the TAT-14 cables is shown in the following figure:

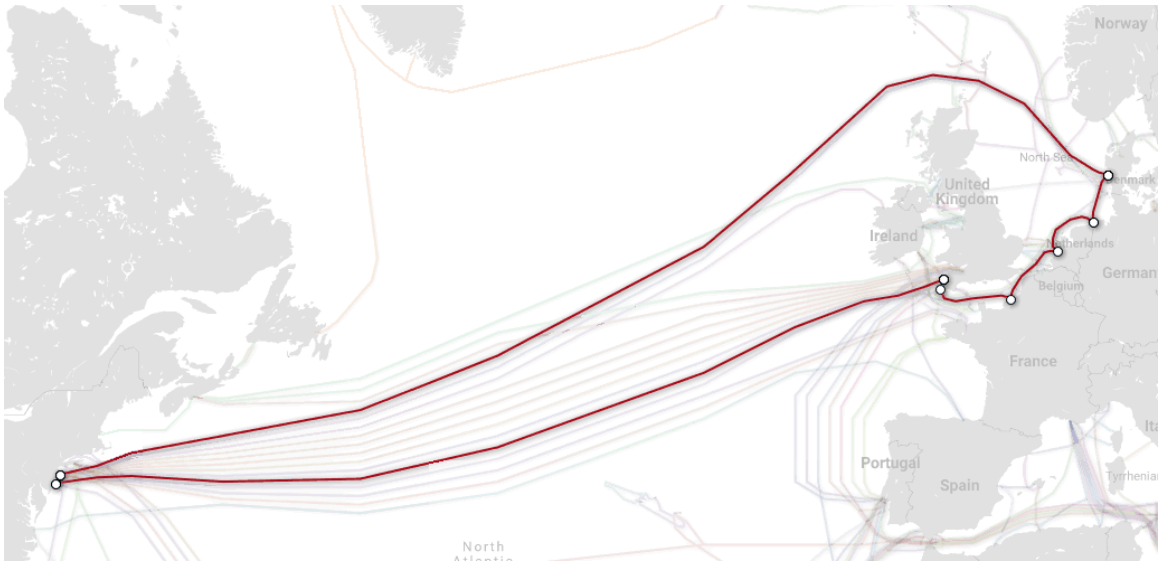


Figure 28 — TAT-14 cable[42]

207. MAREA, a newer cable, installed by Microsoft, Facebook and Telxius (a global telecommunications infrastructure company) that connects the U.S. to Spain, contains 8 pairs of fibers and can support up to 160 Tbps.[43] A map of the MAREA cable is shown in the figure below:

[41] Gigabits per second (Gbps) is a measure of the speed of data transmission. A gigabit is a billion bits of information, and a bit is the smallest unit of digital information, represented by a one or zero. A terabit is 1,000 gigabits. For comparison, 8 bits make up a *byte*, a single text character is represented by a pattern of bits in a byte. A gigabit is enough data to carry about 30 million 4-character words or about 50 copies of Tolstoy's *War and Peace.*

[42] *Submarine Cable Map: TAT-14*, TeleGeography, https://www.submarinecablemap.com/#/submarine-cable/tat-14 (last updated Dec. 6, 2018).

[43] Deborah Bach, *Microsoft, Facebook and Telxius Complete the Highest-Capacity Subsea Cable to Cross the Atlantic*, Microsoft (Sept. 21, 2017), https://news.microsoft.com/features/microsoft-facebook-telxius-complete-highest-capacity-subsea-cable-cross-atlantic.

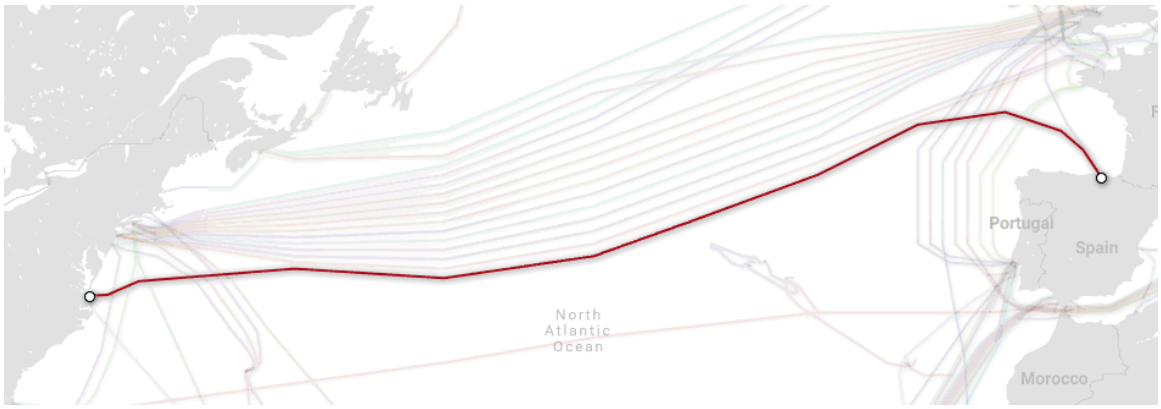


Figure 29 — MAREA[44]

208. The number of fiber pairs in the undersea cables terminating in the U.S. ranges from 4 to 12 (with BICS being the only cable with 12 pairs, and only 4 cables having 8 pairs).[45]

209. Attached as Appendix J is a list of the international undersea cables that terminate in the U.S.[46] The list was compiled from the information on the TeleGeography website.

210. The above description is consistent with the government's description of the submarine cables:

> *The NSA Defendants respond further that, according to data available from Telegeography, international submarine cables typically contain 2-8 pairs of fiber-optic cables. Each fiber-optic pair is typically capable of carrying between approximately 15 and 120 individual communications circuits on different light wavelengths, depending on age and technology used. As a result, an individual submarine cable may carry between approximately 30 and 960 communications circuits. (Individual circuits*

[44] *Submarine Cable Map: MAREA*, TeleGeography, https://www.submarinecablemap.com/#/submarine-cable/marea (last updated Dec. 6, 2018).

[45] *Submarine Cable Map 2018*, TeleGeography, https://www.submarinecablemap.com.

[46] Appendix J (Report on International Submarine Cables Landing in the US, TeleGeography (Jan. 2018)).

> *may be subdivided further to create multiple "virtual circuits" through application of various technologies.) Each wavelength carried on a fiber-optic pair is typically capable of transporting between 10 and 100 gigabits of data per second (10-100 Gbps), meaning that a typical submarine cable can carry between approximately 300 and 96,000 Gbps of data.*[47]

211. Devices at the transmitting end of a fiber use electronics to convert packets into modulated beams of light at specific frequencies (a.k.a., lambdas), and they then use optics to combine multiple lambdas into a single beam of light to send onto the fiber. Devices at the receiving end of a fiber use optics to split the beam of light from the fiber into the individual lambdas, and they then use electronics to reconstitute streams of packets from each of the lambdas.

2. Details of Terrestrial Fiber-Optic Cables

212. Terrestrial fiber-optic cables, ones that cross borders or ones that are a part of an ISP's infrastructure, are much shorter than undersea cables and tend to have far more fibers but, otherwise, operate in the same way that undersea cables do.

3. Public Internet Communications on International Fiber-Optic Cables

213. An individual company can own or lease a whole cable, pairs of fibers within a cable or pairs of lambdas within fibers. In some cases, the cable, fibers or lambdas are owned or leased by ISPs and used as part of the ISP's internal network, as circuits for peering with another ISP or as circuits to Internet exchange points. In the cases where the circuits are connecting to another ISP or to an exchange point, all communications on the circuit would be what I will call in this report ***public Internet***

[47] Appendix H at 4-5 (NSA Response to Plaintiff's Request for Admission No. 1 (Jan. 8, 2018)).

communications or ***public Internet traffic***. That is, communications between Internet users. In the case where the circuit is used as part of the ISP's own network, some of the communications will be to support the ISP operations—to manage their routers for example. These communications would not be considered public Internet communications, while the rest of the traffic on such an internal communications link would be public Internet communications since it would be between Internet users.

214. Not all of the fibers in these cables are used for public Internet communications. Some of the undersea cables, fibers or lambdas are owned or leased by companies for use as part of their own internal networks or for corporate telephone and video communications. Communications on these cables would not be considered public Internet communications. In addition, many cables were built with more fiber than were initially required to allow for future expansion and have not yet been made active, or "lit."

215. Thus, public Internet communications are transported on a subset of the lambdas operating as circuits in a subset of the fibers that these undersea cables are capable of supporting. Since many ISPs consider their internal architecture and the number and location of the other ISPs they peer with to be proprietary, the ISPs and cable operators often do not publicly disclose the specific circuits that are used to transport public Internet communications.

216. Internet sites such as TeleGeography have done a very good job of cataloging the undersea cables that tie together countries around the world, but these sites do not break down which circuits on which fibers on which cables are used for public

Internet traffic and which are used for other purposes such as video distribution or internal corporate networks.

217. Viewing the available information, it is reasonable to infer that the distribution of circuits transporting public Internet communications roughly matches the overall distribution of undersea international cables and terrestrial international cables because the cables, in general, connect population centers where large numbers of Internet users live and work.

4. Undersea Fiber-Optic Cable Landing Locations

218. There are 47 sites where the international undersea cables that were identified from the TeleGeography information come ashore in the U.S.[48] Some of the cables come ashore in more than one U.S. location. TAT-14, which has branches that come ashore in two towns about 40 miles apart on the New Jersey shore, is an example of such a cable. When an undersea cable comes ashore, it is run to an enclosure where the individual fibers are broken out of the cable. The fibers can terminate in network devices (such as routers) in such an enclosure as shown in ¶ 23 of Dr. Schulzrinne's declaration, or they could be patched through to another cable that connects that enclosure to a location, such as a data center, where the network devices are located. The second option is shown in the following figure from a Virginia Beach planning presentation for the MAREA cable termination. The figure shows a conduit path from an enclosure at the beach where the cable comes ashore to a data center where the network devices are:

[48] See Appendix J for a list of the termination sites.

Figure 30 — Conduit path for MAREA cable[49]

219. International Internet links can terminate at a variety of different types of physical facilities within the U.S. For example, some terminate at patching stations such as the one in Virginia Beach shown in Figure 31 below, cable landing stations such as the one shown in ¶ 23 of Dr. Schulzrinne's declaration, Internet exchange points, peering points, or ISP points of presence.

[49] Appendix CC (City of Virginia Beach Dep't of Info. Tech., *Next Generation Network and Transoceanic Subsea Cable Updates* (Oct. 4, 2017), https://www.vbgov.com/government/departments/communications-info-tech/Documents/NGN-and-Transoceanic-Subsea-Cables.pdf).

Figure 31 — Manhole for fiber patching in Virginia Beach[50]

220. As discussed above in ¶¶ 200-201, the vast majority of the U.S. international Internet communications—i.e., communications that start or end in the U.S. where the other end is outside the U.S.—go through the undersea or terrestrial fiber cables shown in the figures above in ¶¶ 201-204.

5. Terrestrial Fiber-Optic Cable Terminations

221. International terrestrial fiber-optic cables do not require as distinct terminations as do undersea cables. Many of them are simple ISP interconnects or connections to Internet exchanges and are indistinguishable from any other terrestrial fiber-optic cables.

[50] Id.

G. Places to Monitor International Public Internet Communications

222. As can be seen in the figures and discussion above, the U.S. termination points of the circuits carried on international undersea cables (see ¶¶ 218-220), as well as the U.S. ends of the international terrestrial cables (see ¶¶ 200, 216, 221) are prime locations to monitor communications between Internet users in the U.S. and Internet users in other countries, because essentially all of the public Internet communications between the U.S. and other countries flow over these circuits.

223. U.S. ends of the circuits carried on the trans-Atlantic and trans-Pacific cables are also attractive places to monitor public Internet communications between some non-U.S. and non-U.S. sites (other than Mexico and Canada). As can be seen from Figure 26, there is only one 2-pair fiber cable connecting South America to Europe and there are no cables connecting South America or the Caribbean with the Far East. Thus, almost all public Internet communications passing between South America, the Caribbean and the rest of the world will pass through the U.S. The same is true, but to a lesser extent, for public Internet communications in circuits in undersea cables between the Far East (China, Japan, Taiwan, and South Korea) and Europe. This means that the U.S. ends of the circuits carried on the trans-Atlantic and trans-Pacific cables are prime locations for monitoring public Internet communications between many non-U.S. locations. Monitoring at those locations also means that any monitoring equipment need only be in U.S. territory. Such monitoring locations would generally not capture communications entirely within a region such as communications between Europeans or such as communications between residents of the Far East.

224. As can be seen in the figures above, the total number of international undersea and terrestrial cables is relatively small, and there are even fewer physical locations where the cables terminate because multiple cables terminate at some of the locations. It is certainly not out of the question that the NSA would have been able to deploy upstream collection devices at all of these sites.

225. As I discuss below in ¶ 291, the FISC has confirmed that the NSA does in fact monitor at least some "*international Internet link[s]*",[51] which are the circuits connecting a network node in the U.S. to a network node in a foreign country. This of course makes sense, given that public Internet traffic on international Internet links will consist almost entirely of communications being sent or received (or both) by a node outside the U.S., which is the traffic that the NSA is authorized to monitor under its Section 702 procedures. It is not relevant to my report or to the conclusions I come to what type of facilities or physical locations at which the NSA is monitoring international Internet links; the relevant point is that the NSA is monitoring at least some international Internet links.

226. NSA representative Rebecca J. Richards, during her deposition, did not specifically say that the NSA monitors at the U.S. ends of the circuits carried on the trans-Atlantic and trans-Pacific cables, but she did say that the NSA did monitor at least one "*Internet backbone circuit*",[52] and she agreed that the international undersea cables can be part of the "*Internet backbone*".[53]

[51] Appendix P at 45 (FISC Opinion (Oct. 3, 2011)).

[52] Appendix K at 122:20-123:5 (Transcript of Deposition of Rebecca J. Richards (Apr. 16, 2018)).

[53] Id. at 79:15-20.

227. In several of its officially disclosed documents, the government has confirmed that it conducts upstream collection on multiple circuits. For example, the PCLOB Report states that upstream collection occurs with the compelled assistance "*of the providers*"—plural—"*that control the telecommunications backbone*".[54] The report also states that the providers facilitating upstream collection must "*assist the government in acquiring communications across these circuits*"—again, plural.[55] That said, it seems very obvious, as the PCLOB Report confirms, that the NSA must be monitoring more than one circuit carried on the international undersea cables. The NSA's thousands of surveillance targets are, presumably, in many parts of the world, and so if the NSA monitored only a single circuit in a single international undersea cable, it could not capture many or most of the communications of those geographically dispersed targets. Moreover, asymmetric routing (as discussed above in ¶¶ 197-199) means that monitoring only a single link could only ever capture those packets in a communication going in one direction, and monitoring only a single link could easily miss all of a target's packets if the routing changed as described above in ¶¶ 194-196.

228. Based on the NSA's description of the capability of undersea fiber cables, cited above at ¶ 210, the international undersea and terrestrial cables that terminate in the U.S. are capable of supporting thousands of individual communications circuits. Some fraction of these circuits are used to transport public Internet communications. It may be that the NSA has deployed enough upstream capture systems to provide full coverage of the international circuits that are used to transport public Internet communications, or the

[54] Appendix F at 40 (PCLOB Report at 35); see also id. at 12 (PCLOB Report at 7).

[55] Id. at 36-37.

NSA may have not done so yet. In any case, I find it hard to believe that the NSA has left many such circuits unmonitored considering the high number of surveillance targets, the variety of circuits that targets' Internet communications may travel into and out of the U.S., the variable routing of Internet communications, the importance the government attributes to the upstream collection program, and the NSA's stated desire to be comprehensive in its collection.[56]

H. Locating Network Nodes Using IP Addresses

229. The use of regional assignment of IP addresses coupled with companies which have developed databases of the geographic locations of specific IP address ranges mean that determining where on the globe a network node using a particular IP is located has become quite reliable. One example of a use of such lists is a system that needs to restrict access to copyrighted material for licensing reasons. For example, Apple iTunes is only usable in specific countries. One commercial database of U.S. IP address ranges includes more than 66,000 individual entries.[57]

230. Locating where a network node is in the real world using the IP address in packets sent to or from a network node is generally but not always accurate. A NAT (see ¶¶ 173-174) will make a whole network's worth of network nodes appear to be in a single location even if the network nodes were actually located anywhere on a nation-wide or world-wide enterprise network. In addition, network nodes using VPNs or tunnels (see ¶ 91) will appear to be where the VPN or tunnel ends rather than where the node actually is. Thus, an IP address filter which uses a list of "U.S. IP addresses" to include or

[56] Id. at 10, 123, 143.

[57] *Create Country ACL*, Country IP Blocks, https://www.countryipblocks.net/country_selection.php.

exclude communications to be reviewed will likely exclude some communications that should be included or include some communications that should be excluded from or to U.S. Internet nodes because of the use of VPNs and NATs.

V. NSA'S SECTION 702 COLLECTING OF COMMUNICATIONS

231. The NSA collects copies of communications involving non-U.S. persons under the authority of Section 702 of the Foreign Intelligence Surveillance Act, as amended. As the government has acknowledged, some of the communications also involve U.S. persons.[58] Two of the NSA's collection programs fall under the authorization of Section 702: ***PRISM*** and ***upstream collection***.[59] I will describe both of these programs below.

232. Under these programs the NSA collects, at least, recordings of phone calls and copies of Internet communications, which the NSA refers to as "*transactions*" (see ¶¶ 63-65), as well as metadata about the communications.

233. The NSA stores these copies in multiple NSA systems and data repositories:

> *Communications provided to NSA under Section 702 are processed and retained in multiple NSA systems and data repositories. One data repository, for example, might hold the contents of communications such as the texts of emails and recordings of conversations, while another, may only include metadata, i.e., basic information about the communication,*

[58] Appendix F at 7, 11 (PCLOB Report at 2, 6).

[59] Id. at 12 (PCLOB Report at 7).

> *such as the time and duration of a telephone call, or sending and receiving email addresses.*[60]

234. These NSA systems and data repositories are also referred to collectively as "*Section 702 databases*".[61]

235. NSA analysts use search tools to identify copies of communications that are stored in the Section 702 databases and which may be relevant to a particular investigation.

A. Selectors

236. Both PRISM collection and upstream collection programs make use of ***selectors*** to identify the communications that are to be collected.

237. The following excerpt describes how selectors are determined:

> *Once the NSA analyst has identified a person of foreign intelligence interest who is an appropriate target under one of the FISC-approved Section 702 certifications, that person is considered the target. The NSA analyst attempts to determine how, when, with whom, and where the target communicates. Then the analyst identifies specific communications modes used by the target and obtains a unique identifier associated with the target - for example, a telephone number or an email address. This unique identifier is referred to as a selector. The selector is not a "keyword" or particular term (e.g., "nuclear" or "bomb"), but must be a specific communications identifier (e.g., e-mail address).*[62]

[60] Appendix L at 7 (NSA Director of Civil Liberties & Privacy Office, *NSA's Implementation of Foreign Intelligence Surveillance Act Section 702* at 6 (Apr. 16, 2014) ("DCLOP Report")).

[61] Appendix F at 132 (PCLOB Report at 128).

[62] Appendix L at 5 (DCLOP Report at 4).

238. The May 2, 2011 letter from a Department of Justice official to Judge Bates of the FISC describes the selectors used in the upstream collection program as including "*electronic communication accounts*", "*electronic communication addresses*" and "*electronic communications identifiers*":

> *As previously described to the Court, in conducting upstream collection using electronic communication accounts/addresses/identifiers (hereinafter "selectors") pursuant to Section 702, NSA acquires Internet communications that are to or from a tasked selector, or which contain a reference to a tasked selector.*[63]

239. The December 8, 2011 DoJ, NSA & DNI joint statement notes that accounts can be tasked:

> *Thus although upstream collection only targets Internet communications that are not between individuals located in the United States and are to, from, or about a tasked account, there is some inevitable incidental collection of wholly domestic communications or communications not to, from, or about a tasked account that could contain U.S. person information.*[64]

240. The Privacy and Civil Liberties Oversight Board (PCLOB) July 2, 2014 report provides additional details on what can be a selector and what cannot:

> *The Section 702 certifications permit non-U.S. persons to be targeted only through the "tasking" of what are called "selectors." A selector must be a specific communications facility that is assessed to be used by the target,*

[63] Appendix M at 1 (FISC Submission (May 2, 2011)); *see also, e.g.*, Appendix N at 4-5 (FISC Submission (Aug. 16, 2011)).

[64] Appendix O at 8 (Joint Statement at 7, *FISA Amendments Act Reauthorization: Hearing Before the H. Permanent Select Comm. on Intelligence* (Dec. 8, 2011)).

> *such as the target's email address or telephone number. Thus, in the terminology of Section 702, people (non-U.S. persons reasonably believed to be located outside the United States) are targeted; selectors (e.g., email addresses, telephone numbers) are tasked. The users of any tasked selector are considered targets—and therefore only selectors used by non-U.S. persons reasonably believed to be located abroad may be tasked. The targeting procedures govern both the targeting and tasking process. Because such terms would not identify specific communications facilities, selectors may not be key words (such as "bomb" or "attack"), or the names of targeted individuals ("Osama Bin Laden"). Under the NSA targeting procedures, if a U.S. person or a person located in the United States is determined to be a user of a selector, that selector may not be tasked to Section 702 acquisition or must be promptly detasked if the selector has already been tasked.*[65]

241. Note that the selector **must be a specific communications facility** such as a telephone number for a telephone facility or an email address for an email facility and cannot be some generic word (e.g., "bomb") or someone's name, since neither of these would be an identifier that was specific to a particular communications facility.

242. Most of the documentation the NSA has publicly released only lists telephone numbers and email addresses as examples of selectors. But some of these documents describe selectors as "*electronic communication accounts/addresses/identifiers*".[66]

[65] Appendix F at 37-38 (PCLOB Report at 32-33).

[66] Appendix M at 1 (FISC Submission (May 2, 2011)).

243. Examples of "*electronic communications accounts*" or "*electronic communications identifiers*" could include Twitter handles, Skype, Snapchat, Snow (a Chinese Snapchat), WhatsApp or Instagram IDs, Wikimedia usernames and similar application-specific identifiers or account names. URLs of target websites or services would also meet the description of "*electronic communications addresses*".

244. In theory, IP addresses could be selectors because they are unique identifiers that qualify as "*electronic communication addresses*". It is worth noting however, that there are many circumstances in which IP addresses do not uniquely identify individual Internet users, which might present difficulties for the NSA in using them as selectors, depending on the circumstances. As the FISC summarized the NSA's explanation:

> *Internet communications are "nearly always transmitted from a sender to a recipient through multiple legs before reaching their final destination." June 1 Submission at 6. For example, an e-mail message sent from the user of [redacted] to the user of [redacted] will at the very least travel from the [redacted] user's own computer, to [redacted], to [redacted] and then to the computer of the [redacted] user. Id. Because the communication's route is made up of multiple legs, the transaction used to transmit the communication across and particular leg of the route need only identify the IP address at either end of that leg in order to properly route the communication. Id. at 7. As a result, for each leg of the route, the transaction header will only contain the IP addresses at either end of that particular leg. Id.*[67]

[67] Appendix P at 34-35 n.33 (FISC Opinion (Oct. 3, 2011)).

245. In other words, packets making up the communication on each of these legs would have the IP addresses of the ends of the individual leg in their source and destination IP address fields. Thus, the IP addresses in the packets of the communications could change multiple times between the source and destination.

246. In addition, the IP addresses in the packets that make up email messages sent or received by a mail server on behalf of any of its users will have the same IP address—the IP address of the server—as their source or destination address, and all packets sent to or from the network nodes behind a NAT or VPN will have the NAT's IP address in the packet's source or destination address fields. (See ¶¶ 173-174.)

247. For these reasons, IP addresses will frequently not be effective selectors for identifying the communications of targets. This, in turn, means that it is more likely that the NSA is reassembling communications in order to determine if they contain selectors.

248. The above sorts of identifiers and others would be uniquely identifying in the way that selectors must be, and so could very well be the type of selectors the NSA uses in conducting upstream collection. The NSA has not publicly disclosed whether it uses them, however, and at least with respect to URLs, the NSA refused during its deposition to say whether it uses them as selectors.[68]

[68] Appendix K at 207:6-208-11 (Richards Depo.)

VI. PRISM COLLECTION PROGRAM

249. Although this case is about upstream collection, understanding how PRISM collection works may be useful in understanding the distinguishing features of upstream collection. (Note that the NSA now refers to PRISM collection as "*downstream collection*".) The Privacy and Civil Liberties Oversight Board (PCLOB) described the PRISM process as follows:

> *In PRISM collection, the government sends a selector, such as an email address, to a United States-based electronic communications service provider, such as an Internet service provider ("ISP"), and the provider is compelled to give the communications sent to or from that selector to the government. PRISM collection does not include the acquisition of telephone calls. The National Security Agency ("NSA") receives all data collected through PRISM. In addition, the Central Intelligence Agency ("CIA") and the Federal Bureau of Investigation ("FBI") each receive a select portion of PRISM collection.*[69]

VII. OPINIONS A, B & C: THE NSA'S UPSTREAM COLLECTION PROGRAM INVOLVES COPYING, REASSEMBLING AND REVIEWING INTERNET TRANSACTIONS

250. In the subsections that follow, I explain how the NSA's upstream collection program must work at a technical level, in the monitoring of any particular circuit. As discussed below in ¶¶ 265-329, I conclude that the NSA's upstream collection process must, as a technical matter, involve copying at an absolute minimum the packets constituting the transactions it wishes to review for the presence of selectors. I also conclude that, as a matter of practical necessity, upstream collection involves either:

[69] Appendix F at 12 (PCLOB Report at 7).

a. copying all of the packets flowing on the circuit, so that the packets can be sent to an IP filter to eliminate those that are part of a wholly domestic transaction, if necessary; or

b. copying all of the packets that an IP address filter test determines are not part of a wholly domestic transaction.

251. In either case, at least the packets that are not part of a wholly domestic transaction are copied.

252. **Opinion A:** Thus, it is my opinion that, to conduct upstream collection of international public Internet communications traversing any particular circuit, as this operation has been described by the government, the NSA must be copying at an absolute minimum the packets constituting the transactions it wishes to review for the presence of selectors. Based on other practical necessities I describe below, it is also my opinion that the NSA is almost certainly either (1) copying all packets traversing that circuit or (2) copying all of the packets that an IP address filter test determines are not part of a wholly domestic transaction.

253. As discussed below in ¶¶ 301-309, I also conclude that to determine whether an Internet transaction that passes the NSA's filter contains a selector, the NSA must first reassemble captured packets into transactions.

254. **Opinion B:** Thus, it is my opinion that, in order to review Internet transactions to determine if a selector tasked for collection is present, the NSA must be reassembling the packets of the transactions it intends to review.

255. As discussed below in ¶¶ 310-327, I also conclude that to determine whether an Internet transaction that passes the NSA's filter contains a selector, the NSA must review all of the reassembled copies of Internet transactions by scanning them to determine if the reassembled Internet transactions contain one of more selectors.

256. **Opinion C:** Thus, it is my opinion that the NSA must review the reassembled Internet transactions in order to identify those that include a tasked selector and thus are subject to collection under the upstream collection program.

A. Upstream Collection Program

257. This case concerns the NSA's upstream collection program, also referred to as ***upstream surveillance***.

258. In the following section I will describe the NSA's upstream collection program as it existed in 2015, when Wikimedia filed its amended complaint. Between 2015 and now, the NSA suspended one part of the program—the part referred to as ***about collection***. As I explain further below, ***about collection*** involved the collection of communications that included a selector in the body of the communication and were therefore "about" a target.

259. In summary, the NSA uses the upstream collection program to collect Internet transactions that contain selectors (see ¶¶ 236-248) and that are from or to a non-U.S. person outside the U.S. The actual collection is done by devices that execute a type of what is known as ***deep packet inspection*** (***DPI***). DPI is a well-known and widely used tool used in enterprise and ISP networks to scan network communications for various purposes, including the detection of security threats. Billions of dollars of DPI equipment are sold annually around the world by many different equipment

manufacturers.[70] For example, since 2008, the Department of Homeland Security has been using successive generations of a DPI system—known as EINSTEIN 2 and EINSTEIN 3 Accelerated—to help protect a number of federal agency networks.[71]

1. A Description of NSA's Upstream Collection Program

260. The government has made a number of statements describing the upstream collection program.

a. The PCLOB described upstream collection as follows:

upstream collection . . . occurs with the compelled assistance of providers that control the telecommunications 'backbone' over which telephone and Internet communications transit, rather than with the compelled assistance of ISPs or similar companies.[72]

b. The PCLOB also said that the term "upstream" refers to the fact that the surveillance

does not occur at the local telephone company or email provider with whom the targeted person interacts . . . but instead occurs 'upstream' in the flow of communications between communication service providers.[73]

c. In the March 19, 2014 PCLOB hearing, Rajesh De, General Counsel of the NSA, stated

upstream collection refers to collection from the, for lack of a better phrase, Internet backbone rather than Internet service providers."[74] *In a*

[70] See, for example: *Deep Packet Inspection (DPI) Market Research Report, Analysis, Trends, Market Size Estimations and Forecast to 2022*, Reuters (Sept. 12, 2017), https://www.reuters.com/brandfeatures/venture-capital/article?id=16008.

[71] U.S. Dep't of Homeland Security, *EINSTEIN*, https://www.dhs.gov/einstein (last updated May 17, 2018).

[72] Appendix F at 12 (PCLOB Report at 7).

[73] Id. at 40 (PCLOB Report at 35).

> *declaration, Miriam P. stated "Upstream collection, in contrast, involves the compelled assistance (through a Section 702 directive) of certain providers that control the telecommunications backbone over which telephone and Internet-based communications transit. Unlike PRISM, Upstream collection generally involves the acquisition of certain communications as they traverse the telecommunications backbone.*[75]

261. All of these statements differentiate upstream collection from PRISM collection based on where the surveillance takes place and the manner in which the surveillance is conducted. Whereas PRISM collection involves compelling electronic communications service providers to turn over communications of their users, upstream collection involves compelling telecommunications providers to turn over communications that transit their networks. And whereas PRISM collection involves the collection of communications to or from the government's targets, upstream collection involves the collection of communications to, from, or (until April 2017) "about" the government's targets.

262. The government's public statements concerning the locations at which upstream collection is conducted are somewhat inconsistent. The second PCLOB statement above, ¶ 260.b, describes upstream collection as taking place in the "*flow of communications between communication service providers.*" The other statements, ¶ 260.a & c, refer to upstream collection as occurring on the "*Internet backbone*," which, as discussed above in ¶¶ 150-153, the government defines more broadly as including (1) the high-speed circuits (network links) and routers that are used to interconnect ISPs, (2)

---

[74] Appendix Q at 26:6-8 (PCLOB, Transcript of Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (Mar. 19, 2014)).

[75] NSA Decl. ¶ 7, *Jewel v. NSA*, No. 4:08-cv-04373 (N.D. Cal. Nov. 7, 2014) (ECF No. 300).

the circuits carried on the undersea cables that connect the U.S. with other countries, and (3) the high speed terrestrial network links (circuits) within the U.S. and between the U.S. and other countries, whether the undersea or terrestrial network links are **between ISPs or within an ISP**.

263. In her deposition, the NSA's representative Rebecca J. Richards agreed that the Internet backbone included connections between ISPs and within ISPs.[76]

264. I will assume for this report that upstream collection may take place on circuits either between ISPs or within an ISP.

2. Upstream Collection Process

265. The process followed for upstream collection was described in the PCLOB report as follows:

> *Once tasked, selectors used for the acquisition of upstream Internet transactions are sent to a United States electronic communication service provider to acquire communications that are transiting through circuits that are used to facilitate Internet communications, what is referred to as the "Internet backbone." The provider is compelled to assist the government in acquiring communications across these circuits. To identify and acquire Internet transactions associated with the Section 702–tasked selectors on the Internet backbone, Internet transactions are first filtered to eliminate potential domestic transactions, and then are screened to capture only transactions containing a tasked selector. Unless transactions pass both these screens, they are not ingested into government databases. As of 2011, the NSA acquired approximately 26.5 million Internet transactions a year as a result of upstream collection.*[77]

[76] Appendix K at 47:18-22, 52:16- 53:12, 54:20- 55:7 (Richards Depo.).

[77] Appendix F at 41-42 (PCLOB Report at 36-37).

266. The "*government databases*" mentioned in the above extract are the same ones referred to as the "*Section 702 databases.*" (See ¶¶ 233-234.)

267. Upstream collection program-related documents refer to both screening, as the above extract does, and "*scanning*."[78] I will use the term ***reviewing*** in this report for this function.

268. The extract at ¶ 265 describes a 3-stage upstream collection process, but given the manner in which upstream collection must be conducted (as I explain below), it is clearer to describe upstream collection conceptually as having 5 stages.

a. Stage 1: Copying the Packets

269. As described in ¶ 38, multiple communications are simultaneously run over each Internet circuit by intermingling packets from different communications on the circuit. This is shown in the following figure:

Figure 32 — Packets on a circuit

270. The small rectangles in the above figure represent packets flowing from left to right over a circuit. The different colors represent packets from different communications. For this explanation, the circuit is one of the ones that the NSA refers to as an Internet backbone circuit and is operated by an electronic communication service provider, which I will refer to as an ***ISP***.

271. I refer to a ***monitoring system*** in the section below. By that I mean, one or more devices that perform the processing required to implement upstream collection.

[78] See, e.g., Appendix R at 3, 24 (FISC Submission (June 28, 2011)); Appendix S at 6 (NSA Section 702 Minimization Procedures (2014)); Appendix F at 124 (PCLOB Report at 119).

Some of these devices may be ones designed by the NSA specifically for the upstream collection program. The government has acknowledged using "*NSA-designed upstream Internet collection devices*" in the upstream collection process.[79] Some of the devices may be off-the-shelf networking devices. I do not mean to imply any particular arrangement of such devices by using the term "system."

272. As a technical matter, there are only two possible configurations the NSA could be using to accomplish the copying of transactions necessary for upstream collection:

a. Copying all the traffic on a circuit so that the traffic can be passed on to one or more devices that then isolate the Internet transactions of interest. I will refer to this configuration as the ***copy-then-filter*** configuration.

or

b. Copying a subset of the traffic on the circuit, for example only the packets that are a part of Internet transactions that are not wholly domestic, and then passing the copied traffic on to one or more devices that then isolate the Internet transactions of interest. I will refer to this configuration as the ***in-line filter*** configuration.

[79] Appendix F at 44 (PCLOB Report at 39).

i. Copy-Then-Filter

273. The copy-then-filter configuration is shown in the following figure:

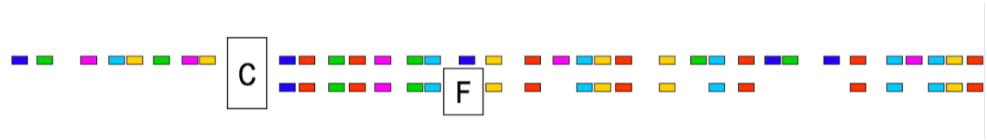


Figure 33 — Copy-then-filter

274. The box marked "C" in Figure 33 represents a device that copies the traffic. The copying in the copy-then-filter configuration could be done in one of two ways; both ways use devices that are placed into a fiber or a circuit:

a. at the physical layer using a fiber-optic splitter;

or

b. at the link layer using a device that makes a copy of all the packets on a circuit.

(1) Fiber-optic splitter

275. A fiber-optic splitter splits the light on a fiber into two parts, each of which is put on its own fiber. Such a splitter could be placed on a fiber carrying traffic from an ISP's terrestrial network into an international cable (Figure 34) or a fiber carrying traffic from an international cable into an ISP's terrestrial network (Figure 35).

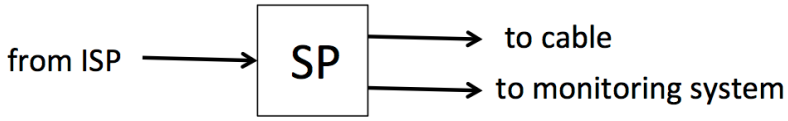


Figure 34 — Fiber-optic splitter on fiber **into** an international cable

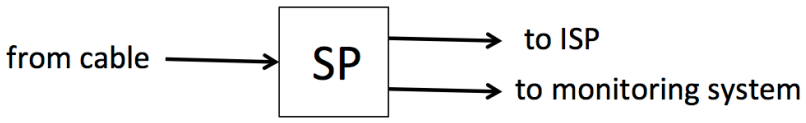


Figure 35 — Fiber-optic splitter on fiber **from** an international cable

276. For the configuration shown in Figure 34, in which the ISP is sending traffic onto the international cable, one fiber from the splitter goes to the international cable and the other fiber goes to the monitoring system. In the other configuration (Figure 35), where the ISP is receiving traffic from the international cable, one fiber from the splitter carries traffic to the ISP, and the other one goes to the monitoring system.

277. In both cases, as discussed above in ¶ 211, the monitoring system must optically split out the lambdas of interest then reconstitute streams of packets from those lambdas. This process results in two copies of the packets: one copy to the ISP or the international cable and one copy to the monitoring system. Dr. Schulzrinne discusses the use of a fiber-optic splitter in ¶ 55 of his declaration.

(2) Link-Layer Copying

278. A link-layer copying of packets can be done by a separate in-line device or by the ISP's router, using for example the router's mirroring function. Dr. Schulzrinne discusses using a router's mirroring function to copy packets in ¶ 58 of his declaration. The use of either a separate copying device or the mirror function in the ISP's router results in all the packets on the circuit being copied and forwarded to the monitoring system.

(3) Filtering the packets

279. The box marked "F" in Figure 33 represents a filtering function in the monitoring system. This filter function can be used to implement the IP address filter

that accepts only Internet transactions that are not wholly domestic, as described in the above PCLOB extract (see ¶ 265) and described below under Stage 2 (see ¶¶ 290-300). The filter function could also be used to implement more extensive filtering.

ii. In-Line Filter

280. In the in-line filter configuration, all the packets on a circuit being monitored by the NSA are sent through an in-line device configured to copy only those packets that meet a set of criteria. This configuration, which is described in ¶ 57 of Dr. Schulzrinne's declaration, is shown in the following figure:

Figure 36 — In-line filter

281. The box marked "F" in Figure 34 represents the filter that (a) copies the subset of the packets on the circuit that meet the filter criteria and (b) sends them on for further processing. Dr. Schulzrinne notes in ¶ 60 of his declaration that the mirroring function in many ISP routers can be configured to perform this filtering function by selectively copying packets based, for example, on access control lists that are configured to use the IP addresses or port numbers in packets.

iii. Implementation

282. For a number of reasons explained below, I consider it most likely that the NSA is using the copy-then-filter configuration implemented using fiber-optic splitters or using link-layer copying. I consider it less likely that the NSA is using an in-line filter and very unlikely that the NSA would be using an in-line filter with sensitive or complex filtering criteria such as those described as possibilities by Dr. Schulzrinne.

283. The copy-then-filter configuration is the easiest configuration for both the NSA and the ISP to implement and operate. This configuration requires no or minimal support from the ISP or its personnel and leaves the NSA in full control of the upstream collection process. All the ISP has to do is to hand the NSA copies of all of the packets on a circuit, which is very easy to do using the router mirroring function, or a portion of the light on a fiber, which is very easy to do with a fiber-optic splitter. Thus the ISP is not a party to any proprietary information other than the basic fact that monitoring is being done at a particular location.

284. In contrast, the in-line filter configuration would require either that the ISP agree to place an NSA-operated device into the heart of its network—unlikely because of the potential impact on the ISP's network in the event of an equipment failure or misconfiguration—or that the ISP's personnel have enough knowledge of the filter criteria to configure the ISP's router.

285. Under Section 702, the NSA can compel an ISP to provide assistance to the NSA as part of upstream collection.[80] Thus, the NSA could compel an ISP to configure its routers to provide the in-line filter functionality. But, compelling an ISP to conduct complex in-line filtering on the ISP's routers would require that ISP personnel know what the NSA's filter criteria were. This would not be a real issue if the filter criteria were not sensitive—for example, if the criteria merely excluded packets with U.S. source and destination IP addresses. But if the filter criteria were more selective, as

[80] 50 U.S.C. § 1881a(i)(1)(A) (Attorney General and Director of National Intelligence may direct that providers "*immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition*").

postulated by Dr. Schulzrinne in ¶ 60 of his declaration, then the ISP personnel would have access to sensitive or classified filtering criteria the NSA uses in its upstream collection process, which I believe the NSA would want to minimize to the greatest degree possible.

286. I do know from personal experience that some parts of the U.S. government consider network device configuration details to be secret. When I was involved in the U.S. government Trusted Internet Connections (TIC) Program as a consultant, I was told that the configurations for the EINSTEIN filtering devices were considered secret because they could disclose what the government knew about cyber attackers.

287. Because of the sensitivity of the filter criteria, I consider it most likely that, if the NSA relies on in-line filters operated by an ISP, the filter criteria would not include blacklisting or whitelisting of individual IP addresses or rejection of individual ports such as 443, because if that information were to ever get out it would provide a roadmap for people who wanted to avoid NSA upstream collection. Note that complex filtering could easily be done using the copy-then-filter configuration, which would not require ISP personnel to have access to the NSA's filtering criteria, because the filter itself would be operated by the NSA.

288. Dr. Schulzrinne suggests that the in-line filter configuration is "*desirable from the perspective of reducing the volume of communications that must be processed (electronically reviewed) to identify the communications of interest*," see Schulzrinne Decl. ¶ 57, but he overstates that benefit. Modern deep packet inspection devices individually or operating in parallel, can process or review Internet communications at

the same rate that those communications traverse high-bandwidth Internet links. In addition, adding even a "simple" IP address-based filter to an ISP's router in order to exclude wholly domestic transactions would require adding tens of thousands of lines to the router's configuration and would place potentially significant additional demands on the router's processing power which could affect the performance of the router and create a risk of overloading the router, thereby interfering with the ISP's ability to support its customers' traffic.

289. In my opinion, the copy-then-filter configuration gives the NSA the greatest operational control and confidentiality in carrying out upstream collection with the least risk of interference with the ISP's ordinary network operations. For these reasons, I consider it more likely that a copy-then-filter implementation is used rather than the in-line filtering that Dr. Schulzrinne hypothesizes. But if an in-line filter is used, in my opinion the filter is almost certainly a simple one as discussed in the next section. (See ¶ 298.) In either case, packets are copied, whether before the filter or by the filter.

b. Stage 2: Filtering

290. The publicly released documents show that the NSA uses IP address filters to eliminate wholly domestic transactions prior to scanning for selectors, though, as explained below, the documents indicate that the NSA may not filter packets by IP address on certain international Internet circuits it is monitoring. The PCLOB extract in ¶ 265 notes that the "*Internet transactions are first filtered to eliminate potential domestic transactions.*"

291. The publicly released NSA documents reveal, however, that not all Internet transactions are filtered to eliminate wholly domestic communications before

being reviewed for the presence of selectors. For example, the NSA's 2014 targeting procedures says:

> *In addition, in those cases where NSA seeks to acquire communications about the target that are not to or from the target, NSA will either employ an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas, or [redacted] In either event, NSA will direct surveillance at a party to the communication reasonably believed to be outside the United States.*[81]

292. The above passage may explain why a wholly domestic "about" transaction could be acquired if the transaction was routed through an international link. Such routing of wholly domestic communications over international circuits does occasionally happen.[82] This situation is described in the following passage from the Foreign Intelligence Surveillance Court's October 3, 2011 opinion describing the operation of the NSA's upstream collection program:

> *the government readily concedes that NSA will acquire a wholly domestic 'about' communication* ***if the transaction containing the communication is routed through an international Internet link being monitored by the NSA*** *or is routed through a foreign server.*[83]

293. This passage indicates that the NSA does not use IP filtering at least on some of the international circuits it is monitoring. This is unsurprising because, by definition, the packets on international circuits are destined for or come from (or both)

---

[81] Appendix T at 2 (NSA Section 702 Targeting Procedure (2014), at 2).

[82] See, e.g., Shaun Waterman, *Internet Traffic Was Routed Via Chinese Servers*, Wash. Times (Nov. 15, 2010), https://www.washingtontimes.com/news/2010/nov/15/internet-traffic-was-routed-via-chinese-servers.

[83] Appendix P at 45 (FISC Opinion (Oct. 3, 2011)) (emphasis added) (citing the government's June 1, 2011 FISC Submission at 29).

non-U.S. locations and thus cannot have U.S. IP addresses as both source and destination addresses except in the case of a routing abnormality.

294. If the NSA were passing all transactions through an IP filter to eliminate wholly domestic transactions before copying, reassembly and review for selectors, then the NSA would never collect a transaction between U.S. IP addresses. That is because the NSA cannot review transactions for selectors, and therefore potentially collect them, without copying the packets and reassembling them into transactions first. (See ¶¶ 301-0.) Since the NSA admits to collecting wholly domestic "about" transactions from international links, it must not be applying an IP address filter in at least those cases. In addition, since the NSA admits it "*will acquire*" wholly domestic transactions from at least some international links, the NSA must be copying, reassembling and reviewing *all* the transactions on those links—otherwise the NSA would not see the selectors in the wholly domestic transactions and would not be collecting them. This is true for upstream collection of communications "to" and "from" the NSA's targets, not just collection of communications "about" its targets.

295. Where the NSA uses an actual IP address filter, it has further described the filtering mechanism as follows:

> *NSA Defendants respond that to their understanding the term "filtering mechanism," as used in the above-referenced brief when filed, meant, in unclassified terms, the devices utilized in the upstream Internet collection process that were designed to eliminate wholly domestic Internet transactions, and transactions that did not contain at least one tasked selector, before they could be ingested into Government databases. Today the term "filtering mechanism" would mean, in unclassified terms, the devices utilized in the Upstream Internet collection process that are*

designed to eliminate wholly domestic Internet transactions, and to identify for acquisition Internet transactions to or from persons targeted in accordance with the current NSA targeting procedures.[84]

296. Most references to the filter function in NSA documents refer to an ***IP filter*** or ***Internet protocol address filter***. An IP filter is a device that can filter Internet packets based on information available in the IP header. The IP header includes a variety of data, but most importantly, it contains the source and destination IP addresses of the packet. (See ¶¶ 96-101.) There are a few places where the NSA refers to its upstream collection filter function as an ***IP address filter***.[85] I believe that the "IP filter" referred to in the other documents is an IP address filter because of these citations and also because the only way that an IP filter could be used to eliminate potential domestic transactions would be to filter based on IP addresses. As discussed above in ¶¶ 229-230, as a general rule, ranges of IP addresses are assigned to ISPs or, through ISPs to their customers in such a way that an individual IP address can be geographically located to a reasonable degree of accuracy. The accuracy is not perfect since blocks of IP addresses are reassigned to different networks in different locations, including in different countries, from time to time. The frequency of these changes has increased significantly in the last few years because of the commercial market for the right to use IPv4 addresses, which I discuss above in ¶ 160. This may be what the NSA is referring to when it says "*[b]ecause NSA's filters will be looking at the best available information*."[86]

[84] Appendix D at 7-8 (NSA Response to Plaintiff's Interrogatory No. 3 (Dec. 22, 2017)).

[85] Appendix U at 24 (FISC Hearing Transcript, *In Re: DNI/AG 702(g) Certification* [*Redacted*] (2008)); Appendix C at 32, 37 (FISC Submission (June 1, 2011)).

[86] See Appendix C at 11 (FISC Submission (June 1, 2011)).

297. Thus, the source and destination IP addresses in each individual packet can be checked to see that both of them are from ranges of IP addresses assigned to a network inside the U.S. Using an IP **address** filter provides the function the NSA described for the IP filter:

> *NSA is required to use other technical means, such as Internet protocol ("IP") filters, to help ensure that at least one end of an acquired Internet transaction is located outside the United States.*[87]

298. Note that even a "simple" filter configured to just reject wholly domestic transactions by using an IP address-based filter is no easy task. There are over 66,000 entries in one of the lists of U.S. address blocks. (See ¶ 229.) Adding and maintaining that many entries to a production router's configuration is a significant task and would have a significant chance of adversely impacting the router's performance.

299. As Dr. Schulzrinne points out in ¶¶ 60-64 of his declaration: In general, such a filter could also be configured to perform other checks such as rejecting any packets transporting protocols that an entity is not interested in, or the reverse, accepting any packets transporting protocols the entity is interested in. The filter could also be configured to reject packets destined to or from particular network addresses an entity might not want to monitor. It should be noted that the more complex the filtering configuration, the more effort is required to keep the filter configurations up to date. As discussed above in ¶¶ 285-289 doing any filtering other than simple U.S. vs. non-U.S. addresses would likely have to be managed by NSA personnel on an NSA operated device or by ISP personnel with security clearances.

[87] Appendix F at 43 (PCLOB Report at 38).

300. To state the obvious, filtering out packets at this stage would eliminate the NSA's ability to collect the Internet communications to which those packets belong, and would thus foreclose its ability under this program to collect and analyze any foreign intelligence information those communications contain.

c. Stage 3: Reassembling Transactions

301. The next step is to reassemble the packets that make up individual communications so that they can be reviewed using DPI for the presence of selectors. As computer researchers Shuhui Chen and Yong Tang put it, "*Stream Reassembly is an indispensable function of Deep Packet Inspection*."[88] What Chen and Tang call a "stream" is another name for what the NSA calls "transactions." (See ¶¶ 63-65.)

302. Transaction reassembly is required before the DPI device can review for selectors because: (1) the packets that make up a particular transaction are intermingled with packets from other transactions (see ¶ 38) and must be isolated from the other packets by selecting the packets with the same source and destination address and ports and the same protocol value (the 5-tuple) and adding them to an assembly buffer[89] (see ¶ 113), (2) the packets may also have to be reordered to be in the right sequence (see ¶ 114), and finally, (3) the selectors that the NSA's reviewing devices look for may be split between the packets that make up the transaction.

[88] Appendix V (Shuihui Chen & Yong Tang, *A Stream Reassembly Mechanism Based on DPI*, Inst. of Electrical & Electronics Engineers (2012)).

[89] By ***assembly buffer***, I mean a temporary storage place in the collection device's memory

303. There are DPI designs that can review for keys such as the NSA's selectors without reassembling the streams (transactions),[90] but since the NSA does need the reassembled transactions to be able to store any with selectors in its databases, transaction reassembly is required even if the reviewing process itself does not need to work on reassembled transactions.

304. The reassembly process is shown in the following figure:

Figure 37 — Reassembling transactions

305. The figure above shows the packets that were passed by the filter being reassembled into Internet transactions. Each transaction comprises all of the packets related to a particular communication (i.e., that have the same 5-tuple) that pass by the monitoring point.

306. The assembly needs to continue until there is an indication that the Internet transaction is complete or there has been some period during which no new packets with a matching 5-tuple have been received.

307. Since the Internet does not guarantee that the order of packets will be maintained during their journey through the network, packets in the buffer may have to be swapped around so that the packets making up the transaction are in the right order. This is required so that any selector that extends across a packet boundary will be made whole for the reviewing process (see below) and be properly recognized.

[90] See, e.g., Appendix W (U.S. Patent No. 8,813,221).

308. Because the paths taken by successive packets as they travel through the network may occasionally change, there is no guarantee that all the packets that make up an Internet transaction will pass by any particular monitoring point. (See ¶ 194.) This will result in some incomplete Internet transactions being assembled. An incomplete Internet transaction might not have a complete selector and thus be missed in the collection process. Conversely, even incomplete Internet transactions may contain complete selectors, and those transactions would thus be collected.

309. Also, because of asymmetric routing paths, the packets that make up the Internet transaction in each direction of the bidirectional exchange of packets that make up most Internet communications (see ¶ 111) will generally not pass through the same monitoring point. (See ¶¶ 197-198.) In those cases where a selector appears in both directions of a communication and where the packets in each direction pass through NSA monitoring points, the upstream collection process will result in both Internet transactions being collected, and they can later be associated during the analysis process. But, it would not be common for some types of selectors, such as a source email address, to be present in both directions of an Internet transaction; normally it would only appear in one direction. The effect of asymmetric routing is one more reason that it is likely the NSA has multiple monitoring points.

d. Stage 4: Reviewing Transactions

310. The Internet transactions that have been reassembled from packets that passed the NSA's IP address filter then need to be reviewed for the presence of selectors. This stage is shown in the following figure:

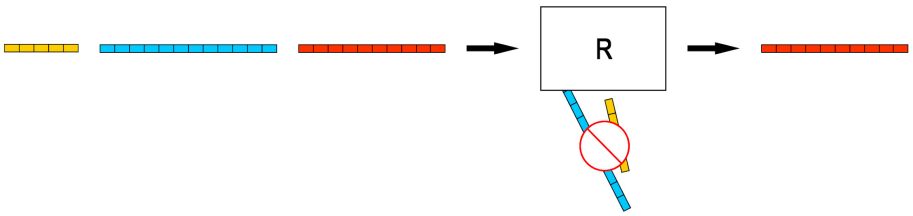


Figure 38 — Reviewing transactions for selectors

311. The above figure shows a series of reassembled transactions being sent to a reviewing device (the box marked "R") and only the transactions containing selectors exiting the device. The remaining transactions are discarded.

312. As discussed above in ¶¶ 236-240, the selectors the NSA uses in the upstream collection program include "*electronic communication accounts/addresses/identifiers*".[91] The examples provided in the NSA documents are account identifiers, telephone numbers and email addresses. These are carried in the application layer in Internet communications. (See ¶ 60.)

313. For example, email addresses are carried in the SMTP handshake (see ¶¶ 134-137), in email headers (see ¶¶ 126-128), in IMAP (see ¶¶ 138-140), and in HTTP/S (see ¶¶ 117-123) when HTTP is the user's interface to an email server (see ¶¶ 129-133). In all of these cases, the email addresses are carried in the application layer of an Internet communication. Email addresses are also sometimes carried in the body of

[91] Appendix M at 1 (FISC Submission (May 2, 2011)).

Internet communications, which is also in the application layer, such as the body of email messages or in the contents of web pages. Telephone numbers in voice over IP are carried in the SIP headers (see ¶ 141), which are also in the application layer. Thus, the NSA must be reviewing the application layer of Internet communications if it is looking for these types of selectors within the communications.

314. In her deposition, Rebecca J. Richards acknowledged that the NSA, at least in 2015, did review the application layer of Internet communications.[92] Following an order from her counsel, she refused to answer the same question about upstream collection today because she said that the answer would be classified.[93] It is strange that the NSA considers classified the answer to the question of whether upstream collection today involves reviewing the application layer of communications. There is no question that it must involve that sort of reviewing, because the email addresses and other user identifiers in Internet communications are transported in the application layer. The NSA has acknowledged using "*NSA-designed upstream Internet collection devices*" in the collection process.[94] The NSA has also acknowledged reviewing web traffic:

> *Results were reviewed for three randomly selected days in April, averaged to produce an estimated figure of collection of [redacted] for the month of April. This figure was then compared to the total take of Section 702 upstream collection of web activity for the month. From this sample NSA estimates that approximately 9% of the monthly Section 702 upstream collection of [redacted].*[95]

---

[92] Appendix K at 263:11-18 (Richards Depo.).

[93] Appendix K at 266:4-13 (Richards Depo.).

[94] Appendix F at 44 (PCLOB Report at 39).

[95] Appendix C at 30 (FISC Submission (June 1, 2011)).

315. ***Web communications*** are the communications carried by HTTP or HTTPS. (See ¶¶ 117-123.) Thus, since the NSA was comparing the amount of collection of a particular redacted type of communication against the amount of collection of "web activity" to get a percentage, they must have been comparing the amount of web (HTTP/S) collection.

i. "multiple communications transaction (MCT)" collection

316. The PCLOB Report described MCT collection as follows:

> *An MCT is an Internet "transaction" that contains more than one discrete communication within it. If one of the communications within an MCT is to, from, or "about" a tasked selector, and if one end of the transaction is foreign, the NSA will acquire the entire MCT through upstream collection, including other discrete communications within the MCT that do not contain the selector.*[96]

317. An example of this type of MCT is the burst of email messages downloaded to a mail user agent when a user reconnects to a mail server after being disconnected for a while. (See ¶ 132.) Under the upstream collection program, the NSA would collect an MCT comprised of multiple email messages if any of the email messages in the burst is from a target outside the U.S. to someone inside the U.S. It might be that only one of the email messages is from the target and ten more are from sources within the U.S., but the entire MCT would be collected.

318. In order to discover that an MCT includes an email message that is from a target, the NSA must be reviewing the entire transaction. This is because each email

[96] Appendix F at 12 (PCLOB Report at 7).

within a burst of email messages has its own header information (e.g., "To:" and "From:" addresses). (See ¶¶ 126-128.)

319. MCT collection is controversial because it can involve the capture of wholly domestic communications, which is generally not authorized under upstream collection. It can also involve the capture of international communications that are not to, from, or about a targeted selector, which again is not generally authorized under upstream collection. But the NSA says that it does not have the technology to separate out the collectable from the non-collectable communications in MCTs.[97]

320. In its April 2017 Order, the FISA Court restricted the NSA to collecting MCTs only "*when the target is a party to the entire MCT*." For example, when the target identified by the selector is in the "To" field of each of the email messages in the MCT.[98]

ii. "about" collection

321. Until April 2017, the upstream collection program collected transactions where selectors appeared **anywhere** in a transaction, not just in the sender or receiver fields of the transaction. For example, upstream collection would collect an email if it contained a selector inside the email message's "body" text. The NSA's "about" collection shows that the NSA was scanning the entirety of each of the reassembled transactions for selectors, likely with the same DPI device that was used to review for other selectors, not just the application headers. (See the discussion above about MCTs.) Prior to April 2017, this scanning led to the ingestion of Internet transactions that were

[97] Appendix F at 45 (PCLOB Report at 40).

[98] Appendix E at 26 (FISC Opinion (Apr. 26, 2017)).

"about" a target in addition to transactions sent by or addressed to a target. The PCLOB Report described "about" collection as follows:

> *An "about" communication is one in which the selector of a targeted person (such as that person's email address) is contained within the communication but the targeted person is not necessarily a participant in the communication. Rather than being "to" or "from" the selector that has been tasked, the communication may contain the selector in the body of the communication, and thus be "about" the selector.*[99]

322. This procedure was controversial because it involved the warrantless reviewing of the contents of Americans' communications and because it involved the collection of many wholly domestic communications where both the sender and receiver of the message were within the U.S. After an extensive review, apparently prompted by the findings of the Foreign Intelligence Surveillance Court that the NSA had not complied with certain procedures related to the upstream collection program, the NSA decided to stop the "about" collection and destroy most of the transactions that had been collected under the "about" collection process.[100]

323. The NSA has not said that it stopped reviewing the entire contents of transactions when it stopped the "about" collection. As mentioned above in ¶¶ 258-259, about collection likely used the same DPI devices that were used to look for communications *to* or *from* a selector, which the NSA still needs to do. "About" collection merely involved retaining transactions with selectors located in parts of a transaction other than in the application headers.

[99] Appendix F at 12 (PCLOB Report at 7).

[100] Appendix X (NSA Press Releases (Apr. 28, 2017)).

324. The recent extension of Section 702 permits the NSA to resume "about" collection under the upstream collection program if it gives proper notice before doing so.[101]

iii. Collection of Encrypted Internet Transactions

325. Under Section 702, the NSA is authorized to collect encrypted Internet transactions and to retain them for an extended period so they can attempt to decrypt them[102]. An HTTPS transaction is an example of an encrypted Internet transaction. In theory, the NSA could configure its IP filters to reject HTTPS traffic by rejecting packets with a destination or source TCP port of 443 but, during her deposition, Rebecca J. Richards followed her lawyer's order to not say if the NSA had done so.[103]

326. In fact, there are obvious reasons that the NSA would seek to collect traffic on port 443 even though it is encrypted.

a. The NSA may, currently or in the future, be able to decrypt important encrypted messages. It is this possibility that justifies the NSA's retention of encrypted communications longer than it is permitted to keep unencrypted communications.[104]

b. For example, the NSA could have compromised the end systems generating or receiving the HTTPS traffic and thus have obtained the keys to permit the transaction to be decrypted. (See ¶ 121.)

---

[101] FISA Amendments Act Reauthorization Act of 2017, Pub. L. No. 115-118, § 103(b).

[102] *See e.g.*, Appendix F at 65, 68 (PCLOB Report at 60, 63); Appendix S at 10 (NSA Section 702 Minimization Procedures (2014)).

[103] Appendix K at 280:13-281:11 (Richards Depo.).

[104] See e.g., Appendix F at 65, 68 (PCLOB Report at 60, 63); Appendix S at 10 (NSA Section 702 Minimization Procedures (2014)).

c. Even if the NSA is not able to decrypt all HTTPS traffic, there is nonetheless useful information that can be obtained from HTTPS transactions including the IP addresses of the Internet user and of the web server. In addition, as discussed in ¶ 123, the domain name of the web server (e.g., www.government.ru) is disclosed in the setup phase of an HTTPS session. In short, even if encrypted, HTTPS communications can reveal who a target is communicating with or which Internet domains he or she is visiting.

d. In addition, as noted in ¶ 109, port numbers are not always a perfect indicator of what application protocol is being used because port numbers can be changed as long as both ends of a communication agree on what port numbers to use. Because of this it is not uncommon for applications to use port 443, the port number assigned for HTTPS, for other uses just to bypass security filters blocking packets using unknown or unwanted ports. Ignoring HTTPS traffic would thus entail ignoring many other types of communications that also use port 443.

e. Finally, HTTPS is one of the most common application-layer protocols used to transmit Internet communications around the world today. Ignoring HTTPS traffic would create a large and needless blind spot.

327. For at least the above reasons, it is very likely that the NSA is reviewing HTTPS transactions whose constituent packets meet the origin or destination criteria for review under upstream collection.

328. Many of the above reasons for collection of HTTPS communications also apply to collecting other forms of encrypted communications, such as communications in

VPNs. For at least these reasons, the NSA would have an incentive to collect encrypted communications of all types.

e. Stage 5: Ingesting Transactions

329. The Internet transactions that pass the reviewing stage are then ingested into the NSA's Section 702 databases. (See ¶¶ 231-235.) The following figure shows this stage:

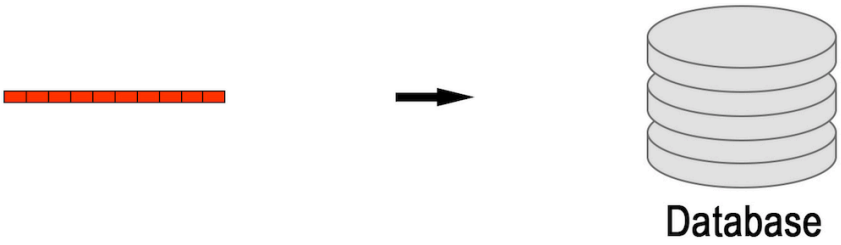


Figure 39 — Ingesting transactions that contain one or more selectors

330. The above figure shows an Internet transaction, in which the reviewing mechanism found one or more selectors, being ingested into the NSA's Section 702 database.

3. Upstream Collection Monitor Placement

331. The NSA has admitted that the upstream collection program collects information from the Internet backbone, and that the Internet backbone consists of high-speed network links between and within ISPs, including terrestrial and undersea fiber cables. (See ¶¶ 150-153.)

332. Since the upstream collection program is limited to collecting Internet transactions where at least one end is outside of the U.S., the logical places to locate upstream collection systems would be at the U.S. end of circuits carried on the undersea and other fiber cables that go between the U.S. and other countries. The FISC, citing the

government's submissions, has confirmed that at least some of the upstream collection program occurs at these points. It has described upstream collection of transactions routed through "*an international Internet link being monitored by the NSA*."[105] As discussed above in ¶¶ 222-223, these locations are also logical places for the NSA to collect communications where both ends are outside the U.S. This non-U.S. collection is feasible because so much of the world's Internet traffic flows through the U.S. (See ¶¶ 222-228.)

333. The NSA has not provided any public information on what percent of the total international public Internet capacity is covered by the upstream collection program, but the government has repeatedly stated that the intention of the upstream collection program is "*to comprehensively acquire communications that are sent to or from its targets*"[106] as long as the communications are not wholly domestic.[107] The NSA refers to the Internet communications it acquires through upstream collection as "*transactions*." (See ¶¶ 63-65.) In order to comprehensively acquire its targets' transactions, the NSA must be comprehensively reviewing Internet transactions to see if they are transactions to or from NSA targets, since the NSA cannot know in advance which of the many transactions on the Internet could be to or from one of the NSA's targets. In order to comprehensively review Internet transactions, the NSA must be comprehensively monitoring the places on the Internet where the non-wholly domestic transactions to or from its targets will transit. If the NSA is not comprehensive in where it does

[105] Appendix P at 45 (FISC Opinion (Oct. 3, 2011)).

[106] Appendix F at 15, 128 (PCLOB Report at 10, 123); see also id. at 148 (PCLOB Report at 143).

[107] Appendix F at 148 (PCLOB Report at 143) ("*[T]he NSA takes additional measures, including the use of IP filters, to try to avoid collecting wholly domestic communications.*").

monitoring, then it cannot be comprehensive in its collection of the transactions to or from its targets. The places where non-wholly domestic transactions to or from its targets will transit include the U.S. ends of the Internet backbone circuits transporting transactions between the U.S. and other countries. (See ¶¶ 200-211.)

334. The NSA has disclosed that it has over 120,000 Section 702 targets, all of them located abroad.[108] The paths that transactions will take between those targets and correspondents in the U.S. are controlled by Internet routing protocols. (See ¶¶ 175-180.) Because of this, in general, the packets that make up these Internet transactions will take the shortest path between the sender and receiver. Using the shortest path will mean that the packets sent by a target located outside the U.S. to a site within the U.S. will generally traverse the topologically closest international link that supports public Internet traffic between the sender's location and the U.S. With thousands of targets in different places around the globe, a wide distribution of international circuits will be used by Internet transactions sent and received by the NSA's targets. In addition, people, including the NSA's targets, move around from time to time, and such movement may change which international circuits their communications use. Thus, the number, distribution and movement of the NSA's targets means that the NSA needs to monitor communications carried by most, if not all, such circuits carried on international cables if it wants to ensure that it captures the communications of those targets.

335. Moreover, regardless of which circuits it monitors, the NSA must also be comprehensive in its monitoring of each circuit. That is, if the NSA's goal is to comprehensively obtain its targets' communications, then it must comprehensively copy,

[108] Appendix Y at 14 (ODNI Statistical Transparency Report for 2017 (Apr. 2018)).

reassemble and review all transactions that could conceivably be to or from a target that transit the circuits being monitored. Since all transactions transiting the monitoring points other than the ones that are wholly domestic could be to or from a target, the NSA must be copying, reassembling and reviewing all, or essentially all, international transactions that transit the circuits being monitored.

VIII. OPINION D: WIKIMEDIA COMMUNICATIONS ARE TRANSPORTED ON ALL INTERNATIONAL CIRCUITS ORIGINATING OR TERMINATING IN THE UNITED STATES.

336. Wikimedia operates servers in multiple countries to optimize the user experience in different regions of the world. This case concerns the international traffic to and from Wikimedia's U.S.-based servers or users, including the communications between Wikimedia's users outside the U.S. and Wikimedia's U.S.-based servers, the traffic between Wikimedia's non-U.S. servers and its U.S-based users, and the international communications of Wikimedia's staff originating in or terminating in the U.S.

337. Comparing the geographic distribution of international undersea and terrestrial cables, which are used to carry public Internet traffic (which I discussed above in ¶¶ 200-204), with the geographic distribution of countries from which users access Wikimedia's U.S.-based servers (which I discuss below in ¶¶ 341-350) makes it clear that communications to and from Wikimedia's U.S.-based servers are carried on all of the circuits transporting public Internet traffic in the cables connecting the U.S. to other countries.

338. **Opinion D:** Thus, it is my opinion that it is virtually certain that Wikimedia's international communications traverse every circuit carrying public Internet traffic on every international cable connecting the U.S. to other countries.

A. Wikimedia

339. Wikimedia Foundation is a non-profit organization based in San Francisco, California, that operates twelve free-knowledge projects on the internet, including Wikipedia, Wiktionary, Wikinews, Wikibooks, and Wikisource. Wikipedia is one of the top ten most-visited websites in the world.[109] Wikimedia describes its mission as to empower people around the world to collect and develop free educational content. Wikimedia does this by developing and maintaining "wiki"-based projects, and by providing the full contents of those projects to individuals around the world free of charge.

340. This case involves Wikimedia's international Internet communications, described more fully below.

1. Wikimedia Websites

341. People all over the world make use of Wikimedia websites. Most users access the websites in order to get information about some topic. For example, Wikipedia is an online free encyclopedia, Wiktionary is an online dictionary, Wikinews is an online news site, Wikibooks is an online repository with open-content textbooks, and Wikisource is an online free library. All of these sites, and seven more, are capable of supporting people around the world in their native languages. For example, as of January 2018, Wikimedia projects supported web pages in 288 languages.[110]

342. In addition, many people around the world volunteer as content producers and editors for Wikimedia services.

---

[109] *The Top 500 Sites on the Web*, Alexa, https://www.alexa.com/topsites.
[110] Appendix Z at 29 (Wikimedia Responses to Defendants' Interrogatories (Jan. 11, 2018)).

2. Wikimedia International Communications

343. Wikimedia operates servers in multiple countries to optimize the user experience in different regions of the world.

344. For purposes of my analysis below, I focus on Wikimedia's web activity, but my conclusions apply to Wikimedia's communications in total. This case concerns three categories of Wikimedia's international communications:

a. Wikimedia's international communications with its community members, which consist principally of the traffic between Wikimedia's users outside the U.S. and its U.S.-based servers, as well as traffic between Wikimedia's U.S.-based users and its Amsterdam-based servers;

b. communications log information sent from Wikimedia's Amsterdam-based servers to its U.S.-based servers[111]; and

c. international communications of Wikimedia's staff that originate in or terminate in the U.S.

345. Wikimedia has maintained servers in the U.S. in the following locations: Ashburn, Virginia; Carrollton, Texas; Chicago, Illinois; Dallas, Texas; San Francisco, California; and Tampa, Florida.[112]

346. For the six-month period between August 1, 2017 and January 31, 2018, Wikimedia engaged in approximately 760 billion international communications.[113] To put the volume of Wikimedia's Internet traffic in comparative perspective, it operates one

[111] According to Wikimedia's discovery responses, "*Every time Wikimedia receives an HTTP/S request from a person accessing a Wikimedia Project webpage, it creates a corresponding log entry*." Appendix AA at 19 (Wikimedia's Second Amended Responses to Defendants' Interrogatories (Apr. 17, 2018)).

[112] Appendix Z at 26-27 (Wikimedia Responses to Defendants' Interrogatories (Jan. 11, 2018)).

[113] Appendix BB Ex. 1 (Wikimedia Response to ODNI Interrogatory No. 19 (Apr. 6, 2018)).

of the top ten most-visited websites in the world, alongside Google.com, Youtube.com, Facebook.com, and Baidu.com.[114]

347. Not only is the volume of Wikimedia's communications immense, but its millions of users are widely dispersed around the globe. For example, Internet users in every country accessed Wikimedia's U.S.-based servers between August 1, 2017 and January 31, 2018. During that time period, Internet users outside the U.S. made over 380 billion web requests to Wikimedia's servers inside the U.S., and Wikimedia's servers sent over 380 billion responses to those requests. See Appendix BB[115] and the map below:

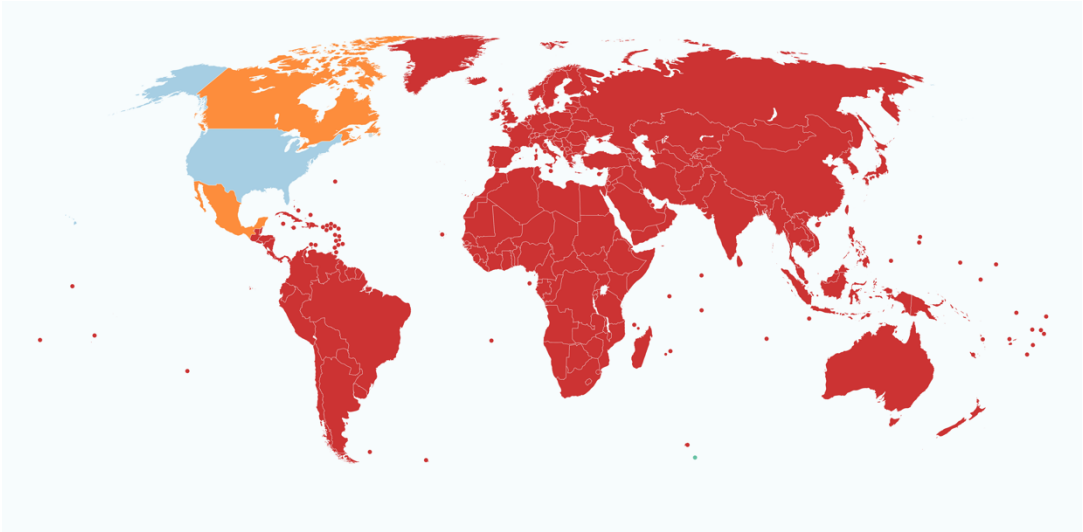


Figure 40 — Countries from which Wikimedia's U.S. servers received web requests

348. Wikimedia's U.S.-based servers receive web requests via circuits in undersea cables from all the countries colored in red. The websites also receive web requests via terrestrial as well as undersea and under-lake circuits from Canada and Mexico, shown in orange. In summary, Wikimedia U.S.-based servers receive web

[114] *The Top 500 Sites on the Web*, Alexa, https://www.alexa.com/topsites.

[115] Appendix BB (Wikimedia Response to ODNI Interrogatory No. 19 (Apr. 6, 2018)).

requests from all of the world's inhabited continents and islands. Thus, Wikimedia users are very widespread. To provide some context, Wikimedia's U.S.-based servers receive hundreds of billions of requests annually and provide at least as many responses. Even with a large number of international circuits, there are very many Wikimedia communications on each circuit. For example, even if there are thousands of international circuits, there would still be hundreds of millions of Wikimedia communications on the average circuit.

349. The paths that Internet communications take between Wikimedia users outside the U.S. and Wikimedia servers in the U.S. are controlled by Internet routing protocols. (See ¶¶ 175-180.) Because of this, in general, the packets that make up these Internet communications will take the shortest path between the sender and receiver. Using the shortest path will mean that the packets sent by a user located outside the U.S. to a server within the U.S. will generally traverse the topologically closest international circuit that supports public Internet traffic between the user's location and the U.S. With Wikimedia users located in all of the world's inhabited continents and islands, the widest possible distribution of international circuits will be used by Internet communications sent and received by the Wikimedia users.

350. Thus, it is my opinion that it is virtually certain that Wikimedia's international communications traverse every circuit carrying public Internet traffic on every international cable connecting the U.S. to other countries, including the "international Internet links" monitored by the NSA.

3. Protocol Support on Wikimedia Websites

351. Wikimedia websites support both HTTP and HTTPS. Within Wikimedia's foreign-to-U.S. HTTP and HTTPS communications, the percentage of communications that use HTTPS had been growing and is now about 97.7% overall.[116] But there are a number of countries where the percentage is much lower. For example, 38% of Iranian communications with Wikimedia's U.S.-based servers use HTTP, as do 28% of Irish communications, 24% of Chinese communications, 19% of Dutch communications, and 16% of Finnish communications (all with Wikimedia's U.S.-based servers).[117] To provide context, Wikimedia's U.S.-based servers received over 8 billion HTTP requests from foreign users in the six months between August 1, 2017 and January 31, 2018.[118]

352. As discussed above in ¶¶ 122, 326, even encrypted Internet transactions can still reveal important information or can be saved for later attempts at decryption. In other words, just because a communication is encrypted does not mean that the NSA will not copy, scan or collect it.

IX. OPINION E: THE NSA HAS COPIED, REASSEMBLED AND REVIEWED WIKIMEDIA COMMUNICATIONS

353. Based on my conclusions above in Opinions A–D, as well as the other features of upstream surveillance I've discussed, I conclude that: Even if the NSA were monitoring only a single circuit under upstream collection, it would be copying and

[116] Appendix AA (Wikimedia's Second Amended Responses to Defendants' Interrogatories (Apr. 17, 2018)).

[117] Id.

[118] Appendix BB, Exhibit 1

reviewing at least some of Wikimedia's communications. Moreover, while it is unnecessary to my conclusion here, the government's officially released documents indicate that the NSA is monitoring multiple circuits, which only increases my confidence that the NSA is copying and reviewing Wikimedia's communications. In fact, for the reasons discussed above in ¶¶ 332-333, the NSA is very likely to be monitoring a large number of international circuits, given that it would need to monitor **most, if not all,** such circuits to accomplish its stated (and unsurprising) goal of reliably and comprehensively collecting the communications of its targets.[119]

354. Moreover, the NSA's need to monitor most, if not all, communications carried by international circuits in order to comprehensively acquire its targets' communications makes it highly likely that the NSA is copying and reviewing some of Wikimedia's communications in each of its categories of international communications. (See ¶ 343.)

355. The NSA's monitoring of many circuits would only increase the volume of Wikimedia communications that the government is intercepting, copying and reviewing in the course of its upstream collection program.

356. **Opinion E:** Thus, it is my opinion that it is virtually certain that the NSA has, in the course of the upstream collection program, copied, reassembled and reviewed at least some of Wikimedia's communications.

[119] Appendix F at 15, 128, 148 (PCLOB Report at 10, 123, 143)

X. DR. SCHULZRINNE'S DECLARATION

357. The government submitted a declaration by Dr. Henning Schulzrinne in support of its motion for summary judgment. Dr. Schulzrinne is a computer scientist at Columbia University. I have known him for many years having first met at the IETF. The government appears to have asked Dr. Schulzrinne to address a different question than Wikimedia's counsel asked me to address. Wikimedia's counsel asked me to address the likelihood that the NSA has, in the course of upstream collection, copied, reassembled or reviewed at least some of Wikimedia's communications. Dr. Schulzrinne's declaration does not address that question. He does not state any opinion about the likelihood that the NSA has copied, reassembled or reviewed Wikimedia's communications.

358. Nor does Dr. Schulzrinne mention many of the critical features of upstream collection on which I base my conclusion that it is a virtual certainty that the NSA has copied, reassembled or reviewed at least some of Wikimedia's communications.

359. For example, he does not address the number of targets of Section 702 surveillance that the government has acknowledged (over 120,000 as of April 2018); he does not acknowledge the NSA's stated goal of "*comprehensively acquir[ing] communications that are sent to or from its targets*";[120] he does not discuss the asymmetric routing of communications on the Internet; he does not mention the special permission the NSA has under Section 702 to collect and analyze encrypted communications; he does not acknowledge that useful information can be obtained from

[120] Appendix F at 15 (PCLOB Report at 10).

the scanning of encrypted Internet communications even if their content cannot be decrypted; and he does not acknowledge that the NSA has publicly conceded that it monitors "*web activity*."

360. In his declaration, Dr. Schulzrinne makes one point about how surveillance can be performed on the Internet, and one about how the NSA could avoid Wikimedia traffic.

361. In regards to the mechanisms of surveillance, Dr. Schulzrinne describes (as I also describe) that there are two configurations of equipment with which the NSA could be obtaining copies of the Internet communications it will review for selectors. Dr. Schulzrinne states that the second configuration (what I call an ***in-line filter***, see ¶¶ 279-281) "*would be desirable*."[121] I disagree with his conclusion. (See ¶¶ 288, 363-365.)

362. Second, Dr. Schulzrinne speculates that the NSA could, as a technical matter, filter out some types of communications so that its surveillance equipment would not copy, reassemble or review any of Wikimedia's communications. Dr. Schulzrinne's explanation is not entirely accurate as a technical matter, and it is simply implausible as a practical matter given everything that is known about upstream collection. (See ¶ 367.)

A. Surveillance Configurations

363. Dr. Schulzrinne describes the same two surveillance configurations as I do. I referred to them as the ***copy-then-filter*** and the ***in-line filter*** configurations. (See ¶¶ 269-289.) Dr. Schulzrinne says that the in-line filter configuration would be desirable as compared to the copy-then-filter configuration because it would reduce the volume of communications that would need to be scanned. As I mentioned above in ¶ 288, I do not

[121] Schulzrinne Decl. ¶ 57.

think that reducing the volume of communications is all that important because modern DPI equipment can, either singularly or in parallel, keep up with the traffic in the type of channels the NSA is dealing with. To the extent that such an in-line filter would permit cheaper DPI equipment to be used, it might be desirable, but there are other important countervailing factors, as described below.

364. Dr. Schulzrinne describes the filtering being done using the mirror function in the ISP's existing routers. If that were the case, it would avoid the need for extra network equipment (the fiber-optic splitter) that would be required in the copy-then-filter configuration. But, as I discuss above in ¶ 287, if the filter function is implemented using the mirror function in the ISP's router, the filter functions would likely have to be limited to some non-secret set of filters such as the list of IP address ranges that are located in the U.S. Otherwise the ISP technician who configures the router, the router itself and the backup systems used to manage the router would be dealing with secret information (the filter criteria), which, if it were to be compromised, would give a roadmap on how to avoid NSA collection. The copy-then-filter configuration has the advantage that the filter device could be entirely under the control of the NSA and thus avoid the risk of the ISP personnel having access to potentially secret filter configurations.

365. In the copy-then-filter configuration, all Wikimedia traffic that transits a channel that the NSA is monitoring will be copied. In the in-line filter case, unless the filter was set to filter with a higher degree of selectiveness than checking to see if the IP addresses are in the U.S. or not then all international Wikimedia traffic that transits a

channel that the NSA is monitoring will be copied. In both cases all international Wikimedia traffic would be copied.

B. Selectively Filtering Internet Traffic

366. Dr. Schulzrinne spends considerable time discussing the possibility that the NSA could use selective filtering to avoid Wikimedia traffic. He describes using the traffic mirror function present in some ISP routers to blacklist or whitelist IP addresses or protocols.[122] While such filtering is technically possible, there are a number of reasons to conclude that Dr. Schulzrinne's hypotheticals are implausible and, accordingly, that it is implausible that the NSA is engaging in such filtering.

a. As discussed above in ¶¶ 285-289, having the mirror function in the ISP router do advanced selective filtering would mean that the configuration of the mirror function would include secret information, complicating the protection of such information.

b. Adding any protocol specific blocklist, for example not including any packets with port 443 (HTTPS) or protocol 50 (IP Sec) in reassembly and review, would create a blind spot that would provide a path by which an NSA target could communicate without the communications being detected. Sophisticated targets could easily probe to find any such blind spots and exploit them.

c. As discussed in ¶ 288, there is no particular reason to think that selective filtering is needed to reduce the load on the DPI devices. In any case, while the total number of Wikimedia's mostly text-based communications is immense, the total amount of those communications in bytes is minuscule as

[122] Id. ¶¶ 63-71.

compared to YouTube's video-based traffic. If filtering traffic for performance reasons were desirable, the NSA would get much more result from filtering YouTube than from filtering Wikimedia.

d. Dr. Schulzrinne mentions using ***whitelists*** (lists of addresses the NSA is interested in) rather than ***blacklists*** (lists of addresses the NSA wants to ignore).[123] As a practical matter, whitelists are almost useless for the type of collection program the NSA is running. Whitelisting requires knowing in advance all of the IP addresses that might be used by each of the NSA's targets as well as assuming that those targets are not moving around and thereby changing their IP addresses. This is not remotely possible. (See ¶¶ 137, 140, 173-174, 229-230, 244-247, 334.)

e. Dr. Schulzrinne suggests selectively filtering applications, for example by using the port number in the transport header.[124] As I discuss in ¶ 109, the use of a particular port number does not mean that a particular application is being used. Port numbers are only advisory in that pairs of Internet devices can decide what application they want to run on a port—for example, running email using port 80 to avoid firewalls. If the NSA were blacklisting traffic using specific ports, it would provide another path that NSA targets could use to avoid collection.

[123] Id. ¶¶ 65-66.

[124] Id. ¶¶ 70-71.

f. One example application Dr. Schulzrinne suggests could be blacklisted is the world wide web (ports 80 and 443).[125] Doing so would leave a very large hole in the NSA's collection ability. The hole would include web email, web chat, web-based editors which have been used to send hidden messages, ISIS videos and the like. In addition, the NSA acknowledges collecting web traffic.[126] (See ¶¶ 314-315.)

g. Dr. Schulzrinne specifically suggests blacklisting HTTPS (port 443). As mentioned just above, the fact that a communication uses port 443 does not mean that the communication is actually HTTPS or even that the communication is encrypted. In addition, as I discuss above in ¶ 326, there are many obvious reasons to believe the NSA is acquiring HTTPS communications, including the fact that the NSA is expressly authorized to collect encrypted Internet communications, and that one can learn a lot from an encrypted HTTPS session, including the IP addresses of the user and server and the domain name of the server.

h. Even if the NSA were blacklisting HTTPS, it would still be virtually certain that the NSA would still be copying, reassembling and reviewing Wikimedia HTTP communications considering the number and distribution of those communications. (See ¶ 351.)

[125] Id. ¶ 79.

[126] Appendix C at 30 (FISC Submission (June 1, 2011)).

C. Selectively Filtering Wikimedia IP addresses

367. Dr. Schulzrinne posits that the NSA could "blacklist" Wikimedia's IP addresses and suggests that if the NSA did so, "*NSA would receive no access to Wikimedia HTTP or HTTPS communications (or, for that matter, Wikimedia communications of any kind)*" (Schulzrinne Decl. ¶ 81). As I show below, that claim is technologically inaccurate and entirely implausible. Dr. Schulzrinne concedes that he has no evidence to support the possibility that the NSA made such a decision, and he does not offer his view on the **likelihood** that the NSA would make such a decision; he merely claims that it is technically possible.[127]

a) In my opinion it is basically inconceivable that the NSA would have decided to blacklist Wikimedia IP addresses. Given that there are millions of websites on the public Internet, the idea that the NSA would have gone through them to decide which to monitor and which not to, in addition to being an incredibly resource-intensive task, is just totally unbelievable. Any such blacklist would purposefully create blind spots in the upstream collection program that could be exploited by NSA targets to bypass surveillance. Including Wikimedia IP addresses in any such blacklist would deliberately limit the possible collection of information on the use of Wikimedia resources by NSA targets, a potentially valuable source of information about the online research and reading of its targets. Viewed in total, taking into account the total lack of any evidence supporting the possibility that the NSA took such action, the idea that the NSA made a deliberate decision to avoid Wikimedia communications seems entirely implausible.

[127] Schulzrinne Decl. ¶ 77

b) It is also technologically incorrect that blocking Wikimedia's IP addresses would block all Wikimedia traffic. Even if NSA blacklisted Wikimedia's IP addresses, Wikimedia's communications would still be copied, reassembled and reviewed by the NSA in at least several circumstances:

(1) MCTs that contain Wikimedia communications, where the enclosing communication is not to or from Wikimedia, but one or more of the embedded communications are to or from Wikimedia.

(2) In the case where a person located outside the U.S. is using an email service located inside the U.S. to send email to Wikimedia. The first "leg" of the journey the email takes from the user's mail agent to the email server would be subject to copying, reassembly and review because the transaction carrying the email message is not wholly domestic. The same is true in reverse: email from Wikimedia to such a person outside the U.S. would not be seen as wholly domestic in the leg between the email service and the user's mail agent. In both of the above cases, the email transaction transiting the international circuit would not have any Wikimedia IP addresses in the IP headers of the packets such that they could be discarded by an IP address-based blacklist.

(3) The traffic between a VPN service in the U.S. and a user located outside the U.S. would not have Wikimedia IP addresses in the traffic even if the user were accessing a Wikimedia site.

c) In any case, the NSA's descriptions of its IP address filtering all state that the goal is to filter out "*wholly domestic communications*,"[128] and these descriptions do not contain any mention of any other goals for the filtering.

D. U.K. Surveillance Disclosures and Court Proceedings

368. The U.K.'s signals intelligence agency, Government Communications Headquarters (GCHQ), is charged with performing the functional equivalent of upstream collection in the U.K.[129] GCHQ's public disclosures reinforce my conclusion that, for various technical and practical reasons, the NSA copies the entire stream of communications on a circuit it is monitoring. The GCHQ has explained in court filings that, for "*technical reasons*" and "*as a matter of practical necessity*," it needs to intercept the entire stream of communications on a circuit (which GCHQ refers to as a "*bearer*") when engaging in its equivalent of upstream collection:

> *As explained in detail in the Observations, the s.8(4) Regime operates in this way as a matter of practical necessity. For technical reasons, it is necessary to intercept the entire contents of a bearer, in order to extract even a single specific communication for examination from the bearer: Observations, §§1.31-1.34.*[130]
>
> *Subjects of interest are very likely to use a variety of different means of communication, and to change those means frequently. Moreover, electronic communications do not traverse the internet by routes that can*

[128] Appendix D at 7-8 (NSA Response to Plaintiff's Interrogatory No. 3 (Dec. 22, 2017)); Appendix F at 46, 125, 148 (PCLOB Report at 41, 120, 143); Appendix H at 7-8 (NSA Response to Plaintiff's Request for Admission No. 6 (Jan. 8, 2018)).

[129] Appendix DD ¶ 12 (*Case of Big Brother Watch & Others v. United Kingdom*, Eur. Ct. H.R., ¶ 12 (2018), http://hudoc.echr.coe.int/eng?i=001-186048).

[130] Appendix EE ¶¶ 7-8 (Further Observations of the Government of the United Kingdom ¶¶ 7-8, *10 Human Rights Organizations v. United Kingdom*, Eur. Ct. H.R. (Dec. 16, 2016), https://privacyinternational.org/sites/default/files/2018-02/2016.12.16%20Government%27s%20further%20obs.pdf).

> *necessarily be predicted. Communications will not take the geographically shortest route between sender and recipient, but the route that is most efficient, as determined by factors such as the cost of transmission, and the volume of traffic passing over particular parts of the internet at particular times of day. So in order to obtain even a small proportion of the communications of known targets overseas, it is necessary for the Services to intercept a selection of bearers, and to scan the contents of all those bearers for the wanted communications.*[131]

369. In its ruling, the European Court of Human Rights repeated this description of how the U.K.'s Internet surveillance program operates.[132] In spite of the fact that the GCHQ may not be operating under the same requirement to exclude wholly domestic U.K. traffic from its collection program, GCHQ's practice—and the reasons it has publicly described—reinforce my conclusions that the NSA relies on the copy-then-filter configuration to conduct the upstream collection program and that it does not selectively filter traffic prior to copying it as Dr. Schulzrinne hypothesizes it could.

370. But even if Dr. Schulzrinne's hypothesis that the NSA is filtering certain traffic before copying the remainder were to be true, for the reasons I set forth above, it is virtually certain that the NSA has, in the course of the upstream collection program, copied, reassembled and reviewed at least some of Wikimedia's communications. This, also for the reasons I set forth above, is also true in the highly improbable scenario that

[131] Appendix FF ¶¶ 1.29-1.31, 4.5-4.6 (Observations of the Government of the United Kingdom, ¶¶ 1.29-1.31, 4.5-4.6, *10 Human Rights Organizations v. United Kingdom*, Eur. Ct. H.R. (Apr. 16, 2016), https://privacyinternational.org/sites/default/files/2018-02/United%20Kingdom%E2%80%99s%20Observations%20on%20the%20Merits.pdf).

[132] Appendix DD ¶ 284 (*Case of Big Brother Watch & Others v. United Kingdom*, Eur. Ct. H.R., ¶ 284 (2018)).

Dr. Schulzrinne hypothesizes that the NSA has been purposefully blacklisting Wikimedia IP addresses from the upstream collection program.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Date: 12/18/18

Scott Bradner

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, *Plaintiff*, v. NATIONAL SECURITY AGENCY / CENTRAL SECURITY SERVICE, *et al.*, *Defendants*.	No. 1:15-cv-00662-TSE

DECLARATION OF SCOTT BRADNER
APPENDIX LIST

Observations of the Government of the United Kingdom, *10 Human Rights Organizations v. United Kingdom*, Eur. Ct. H.R. (Apr. 16, 2016) .....FF

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, *Plaintiff*, v. NATIONAL SECURITY AGENCY / CENTRAL SECURITY SERVICE, *et al.*, *Defendants*.	No. 1:15-cv-00662-TSE

DECLARATION OF SCOTT BRADNER
APPENDIX LIST

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix A

SCOTT BRADNER

WORK EXPERIENCE

- Senior Technology Consultant, Office of the CTO, Harvard University, Cambridge, MA, 2012 to 2016. Exploring, developing and upgrading technology at Harvard, monitoring changing technology trends and exploring their potential for use at Harvard. Last focus was on implementing cloud-based identity and access management applications.
- University Technology Security Officer, Office of the CTO, Harvard University, Cambridge, MA, 2011 to 2012.
- University Technology Security Officer, Office of the CIO, Harvard University, Cambridge, MA, 2008 to 2011. Developed and maintained university IT security policies, assessed compliance with such policies, provided advice on IT security issues.
- University Technology Security Officer, Office of the Assistant Provost for Information Systems, Harvard University, Cambridge, MA, 2004 to 2008. Developed and maintained university IT security policies, assessed compliance with such policies, provided advice on IT security issues.
- Senior Technical Consultant, Office of the Assistant Provost for Information Systems, Harvard University, Cambridge, MA, 1996 to 2008. Assist Assistant Provost in ascertaining the implications of advanced technology on the University, served as a liaison to various University groups dealing with technology issues.
- Senior Technical Consultant, Office for Information Technology (OIT), Harvard University, Cambridge, MA, 1989 to 1996. Design data networks, install and operate production gateways, served as OIT liaison to external organizations, oversee installation of fiber infrastructure, develop network based applications, develop recommendations on security and privacy, document existing Harvard network and network support organization.
- Founded and managed the Harvard Network Device Test Lab, 1988 to 1999.
- Senior Technical Consultant, Psychology Department, Harvard University, Cambridge, MA, 1975 to 1990. Managed computer facility consisting of UNIX computers, PCs and Macintosh computers, developed phototypesetting facility, designed and installed first Harvard campus data network and designed the Longwood Medical Area Network.

- Computer Programmer, Psychology Department, Harvard University, Cambridge, MA, 1966 to 1975. Co-developed real-time operating system and designed special hardware to support real-time research experiments.
- Computer Programmer, Information International Incorporated, Cambridge, MA, 1964 to 1965. Worked on film scanning systems.
- Lab technician, Children's Hospital Cancer Institute, Boston, MA, 1964.

TEACHING

- Instructor, Harvard University Extension School, from 1995 to the present. Teaching classes in *Technology, Security, Privacy, and the Realities of the Cyber World*. Previously taught *Advanced Topics in Data Networking Protocols and Network Architecture* and *Security, Privacy, and Usability*, also at the Harvard University Extension School
- Tutorial Instructor, Networld + Interop, from 1990 to 2001. (Now known as Interop.) Taught classes in multiprotocol enterprise and Internet service provider data networking.
- Tutorial Instructor, IBM Corporation, from 1990 to 1995. Taught classes in advanced TCP/IP data networking.
- Senior Preceptor, Harvard University, 1982 to 1990. Taught classes in the use of computers in psychology and supervised special projects in computer and networking electronics and in computer programming.

CONSULTING

- Consultant on network design, management and security to educational institutions, Federal agencies, international telecommunications enterprises and commercial organizations ranging from Fortune 500 companies to small businesses, 1989 to present. Served as an Expert Witness in a number of legal cases including the Communications Decency Act challenge in the U.S. Federal court.

PATENTS

- US Patent 4,799,262 - *Speech Recognition* (with Joel A. Feldman and William F. Ganong, III) 1989

AWARDS

- The Jonathan B. Postel Service Award from the Internet Society
- The Petra T. Shattuck Excellence in Teaching Award from the Harvard University Extension School

ORGANIZATIONS

Internet Engineering Task Force (IETF)

- Consultant to IAOC and IETF Trust (2016 to present)
- Member, IETF Administrative Oversight Committee (IAOC) of the IETF Administrative Activity (IASA) (2012 to 2016)
- Co-Chair, Operations and Management Area Working Group (opsawg), (2007 to 2016)
- Co-Chair, Authority-to-Citizen Alert Working Group (atoca), (2010 to 2012)
- Co-Chair, Congestion and Pre-Congestion Notification Working Group (pcn), (2007 to 2012)
- Co-Chair, Internet Emergency Preparedness Working Group (ieprep), (2002 to 2007).
- Liaison between IETF and ITU-T, (1995 to 2009).
- Chair, New IETF Standards Track Discussion Working Group (newtrk), (2004 to 2006).
- Member, IETF Internet Engineering Steering Group (1993 to 2003).
- Co-Director, Sub-IP Area (2001 to 2003).
- Co-Chair, Transport Area Working Group (tsvwg), (1999 to 2003).
- Co-Director, Transport Area (1997 to 2003).
- Co-Director, IPng Area (1993 to 1996).
- Co-Director, Operational Requirements Area (1993 to 1997).
- Chair, Benchmarking Methodology Working Group (bmwg), (1990 to 1993).
- Edited or co-edited many IETF process and IPR documents (RFC 2026, RFC 2028, RFC 2418, RFC 2436, RFC 2438, RFC 2690, RFC 2691, RFC 3113, RFC 3131, RFC 3233, RFC 3356, RFC 3427, RFC 3667, RFC 3668, RFC 3978, RFC 3979, RFC 4053, RFC 4748, RFC 4775, RFC 5378, RFC 6756, RFC 7127, and RFC 7691).
- Maintained and presented IETF newcomers tutorial (2003-2016) (IETF meeting: 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, and 95).
- Editor of most cited RFC (RFC 2119).

Internet Society (ISOC)

- Secretary of the Board (2003 to 2016)
- Vice President for Standards, (1995 to 2003).
- Trustee, (1993 to 1999).

The American Registry for Internet Numbers (ARIN)

- Vice Chair of the Board (2011 to 2012)
- Treasurer (2009 to 2010)
- Secretary of the Board (1997 to 2009)
- Trustee, (1997 to 2012)

IEEE Internet Computing

- Editorial Board, (1999 to 2008).

Wiley Computer Publishing

- Wiley Network Council, (1997 to 2000). Technical editing for a number of books including: Internet Performance Survival Guide, by G. Huston; Converged Networks and Systems, by I. Faynberg; Network Services Investment Guide: Maximizing ROI in Uncertain Times, by M. Gaynor; Network Routing Basics: Understanding IP Routing in Cisco Systems, by J. Macfarlane; The NAT Handbook: Implementing and Managing Network Address Translation, by B. Dutcher; and WAN Survival Guide: Strategies for VPNs and Multiservice Networks, by H. Berkowitz

Corporation for Regional and Enterprise Networking, Inc. (CoREN)

- Co-chair, Joint MCI-CoREN Technical Committee (1994 to 1995)

New England Academic and Research Network (NEARnet)

- Co-founder
- Member, Steering Committee (1989 to 1995)
- Chair, Technical Committee (1989 to 1995)

Longwood Medical Area Network

- Chair, Technical Committee (1991 to 1995)

Technical Advisory Boards

- I have been on over two dozen technical advisory boards over the years.

Member, ACM, IEEE, ISOC

SELECTED PUBLICATIONS

Columns

- *Net Insider*, Network World, 1992 to 2013
- *View from the USA*, Nikkei Communications, 1997 to 1999

Papers and Articles

- Gaynor, M., L. Lenert, K. D. Wilson and S. Bradner, Why common carrier and network neutrality principles apply to the Nationwide Health Information Network (NWHIN), Journal of American Medical Informatics Association, 2013
- Gaynor, M, F. Yu, C. Andrus, S. Bradner and J. Rawn, A General Framework for Interoperability with Applications to Healthcare, Health Policy and Technology, January 2013
- Bellovin, S., S. Bradner, W. Diffie, S. Landau, and J. Rexford., As Simple as Possible - But Not More So, Communications of the ACM, August 2011
- Bellovin, S., S. Bradner, W. Diffie, S. Landau, and J. Rexford, Can It Really Work? Problems with Extending EINSTEIN 3 to Critical Infrastructure, Harvard Law School National Security Journal, May 2011
- Gaynor, M., A. Pearce, S. Bradner, and Ken Post, Open Infrastructure for a Nationwide Emergency Services Network, International Journal of Information Systems for Crisis Response Management (IJISCRAM), 2009
- Gaynor, M., and S. Bradner, Statistical Framework to Value Network Neutrality, Media Law & Policy, New York Law School, March 2008
- Gaynor, M. and S. Bradner, Valuing Network Neutrality, Broadband Properties, December 2007
- claffy, kc, S. Meinrath and S. Bradner, The (un)Economic Internet?, IEEE Internet Computing, May/June 2007
- Bradner, S., The End of End-to-End Security, IEEE Security & Privacy, March/April 2006
- Goodell, G., M. Roussopoulos and S. Bradner, A Directory Service for Perspective Access Networks, Harvard University Computer Science Group Technical Report TR-06-06, 2006
- Goodell, G., S. Bradner and M. Roussopoulos, Building a Coreless Internet without Ripping out the Core, Hotnets05, November 2005

- Bradner, S. and C. Metz, Guest Editor's Introduction: The Continuing Road toward Internet Media, IEEE Internet Computing, July-August, 2005
- Bradner, S., Internet governance - a train on many tracks, ARIN newsletter, December 2004
- Gaynor, M., S. Bradner A Real Options Metric to Evaluate Network, Protocol, and Service Architecture, Computer Communication Review (CCR), October 2004
- McKnight, L., J. Howison, and S. Bradner, Wireless Grids: Distributed Resource Sharing by Mobile, Nomadic, and Fixed Devices, IEEE Internet Computing, July-August 2004
- Goodell, G., S. Bradner and M. Roussopoulos, Blossom: A Decentralized Approach to Overcoming Systemic Internet Fragmentation, Harvard University Computer Science Group Technical Report TR-25-04, 2004
- Kung, H.T., C-M. Cheng, K-S Tan, and S. Bradner, Design and Analysis of an IP-Layer Anonymizing Infrastructure, Proceedings of the third DARPA Information Survivability Conference and Exposition (DISCEX 3), April 2003
- Bradner, S., Are Global Internet-Related Standards Possible?, International Journal of IT Standards and Standardization Research, Jan-Mar 2003
- King, K. and S. Bradner, Internet Emergency Preparedness in the IETF, Applications and the Internet Workshops, Jan 2003
- Kung, H.T., S. Bradner, and K. S. Tan, An IP-layer Anonymizing Infrastructure, MILCOM 2002, Anaheim, CA, October 2002
- Bradner, S., Internet Telephony -- Progress Along the Road, IEEE Internet Computing, May/Jun 2002
- Gaynor, M. and S. Bradner, The Real Options Approach to Standardization, Proceedings of Hawaii International Conference on Systems Science, Jan 2001
- Gaynor, M., S. Bradner, M Iansiti, and HT Kung, The Real Options Approach to Standards for Building Network-based Services, Proceeding of IEEE Conference on Standardization and Innovation in Information Technology, Oct 2001
- Gaynor, M. and S. Bradner, Using Real Options to Value Modularity in Standards, Journal of Knowledge Technology & Policy (Special issue on IT standards)
- Bradner, S., Virtual networking: reflections on the status of ATM, Journal of High Speed Networks, Volume 6, Number 3, 1997

- Bradner, S., The Bradner Report: The yet untold story and barking dogs, Network Computing, Aug 15, 1997
- Bradner, S., The Bradner Report, Network Computing, July 15, 1996
- Bradner, S., The Bradner Report 1995, Network Computing May 15, 1995
- Bradner, S., The Bradner Bridge Report, Network Computing, October 1, 1994
- Bradner, S., The Exclusive Bradner Report, Network Computing, September 1, 1994
- Bradner, S. and D. Greenfield, Building the Highway, PC Magazine, March 30, 1993
- Bradner, S., Rooting out the Best Routers, SunExpert Magazine, October 1992
- Bradner, S., Bridges or Routers: What Matters?, 3TECH The 3Com Technical Journal, Winter 1992
- Bradner, S., Ethernet Bridges and Routers: Faster Than Fast Enough, Data Communications, February 1992
- Bradner, S., Testing Multiprotocol Routers: How Fast is Fast Enough?, Data Communications, February 1991

Books

- Bradner, S., *Forward* in *The Complete April Fools' Day RFCs*, compiled by T. Limoncelli and P. Salus, Peer-to-Peer Communications, 2007, ISBN 13: 978-1-57398-042-5
- Bradner, S., *Forward* in *TCP/IP for Dummies* by C. Leiden and M. Wilensky, Wiley Publishing, 2003, ISBN 0-7645-1760-0
- National Research Council, *The Digital Dilemma*, The National Academies Press, 2000, ISBN: 978-0-309-06499-6
- Bradner, S., *Current Trends in the IETF and Voice over IP*, chapter in *Carrier IP Telephony 2000*, The International Engineering Consortium, 2000, ISBN 0-933-21775-7
- Bradner, S., *The Internet Engineering Task Force*, a chapter in *Open Sources: Voices from the Open Source Revolution,* edited by C. DiBona, S. Ockman & M. Stone, O' Reilly, 1999, ISBN 1-56592-582-3
- Mitchell, D., S. Bradner and K Claffy, *In Whose Domain?: Name service in Adolescence*, section in *Coordinating the Internet*, MIT Press, 1997, ISBN 0-262-11230-2
- Bradner, S., and A. Mankin (Eds.), *IPng, Internet Protocol Next Generation*, Addison-Wesley 1996, ISBN 0-201-63395-7

- Bradner, S., *A Practical Perspective on Routers*, a chapter in *The Internet System Handbook*, Edited by D. Lynch & M. Rose, Addison-Wesley, 1993, ISBN-0-201-56741-5

IETF RFCs and Internet Drafts

- Bradner, S. and J. Contreras, Eds., *Intellectual Property Rights in IETF Technology*, RFC 8179, May 2017
- Bradner, S. Ed., *Updating the Term Dates of IETF Administrative Oversight Committee (IAOC) Members*, RFC 7691, November 2015 ID00, ID01, ID02, ID03, ID04
- Kolkman, O., S. Bradner and S. Turner, *Characterization of Proposed Standards*, RFC 7127, January 2014
- Bradner, S., K. Dubray, J. McQuaid, and A. Morton, *Applicability Statement for RFC 2544: Use on Production Networks Considered Harmful*, RFC 6815, November 2012
- Trowbridge, S., Ed., E. Lear, Ed., G. Fishman, Ed., S. Bradner, Ed., *Internet Engineering Task Force and International Telecommunication Union - Telecommunication Standardization Sector Collaboration Guidelines*, RFC 6756, September 2012
- Bradner, S, L. Conroy & K. Fujiwara, *The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)*, RFC 6116, March 2011 ID00, ID01, ID02, ID03, ID04, ID05, ID06, ID07, ID08, ID09
- Klensin, J. and S. Bradner, *Restoring Proposed Standard to Its Intended Use*, IETF Internet Draft, January 2011
- Arkko, J. and S. Bradner, *IANA Allocation Guidelines for the IPv6 Routing Header*, RFC 5871, May 2010
- Bradner, S. and J. Contreras, Eds., *Rights Contributors Provide to the IETF Trust*, RFC 5378, November 2008, ID00 ID01 ID02 ID03 ID04 ID05 ID06 ID07 ID08 ID09
- Falk, A. and S. Bradner, *Naming Rights in IETF Protocols*, RFC 5241, 1-April-2008
- Arkko, J. and S. Bradner, *IANA Allocation Guidelines for the Protocol Field*, RFC 5237, February 2008
- Bradner, S., B. Carpenter (Ed.), and T. Narten, *Procedures for Protocol Extensions and Variations*, RFC 4775, December 2006
- Bradner, S. Ed., *RFC 3978 Update to Recognize the IETF Trust*, RFC 4748, October 2006, ID00 ID01 ID02 ID03

- Bradner, S., *Obtaining Additional Permissions from Contributors*, Internet Draft, July 2005
- Trowbridge, S., S. Bradner and F. Baker, *Procedures for Handling Liaison Statements to and from the IETF*, RFC 4053, April 2005
- Bradner, S., *IETF Rights in Contributions*, RFC 3979, March 2005, ID00
- Bradner, S., *Intellectual Property Rights in IETF Technology*, RFC 3978, March 2005
- Bradner, S. Ed., *Extracting RFCs*, Internet Draft, February 2005, ID01
- Bradner, S., *Indication of Trademarks in IETF Documents*, January 2005, Internet Draft
- Bradner, S., *Sample ISD for the IETF Standards Process*, Internet Draft, October 2004
- Bradner, S., *Omniscience Protocol Requirements*, RFC 3751, 1-April-2004
- Bradner, S., *Intellectual Property Rights in IETF Technology*, RFC 3668, February 2004
- Bradner, S., *IETF Rights in Contributions*, RFC 3667, February 2004, ID00 ID01 ID02 ID03 ID04 ID05 ID06 ID07 ID08
- Bradner, S., *Ideas for changes to the IETF document approval process*, Internet Draft, July 2003
- Bradner, S., *An Idea for an Alternate IETF Standards Track*, Internet Draft, July 2003 ID01
- Mankin, A., S. Bradner, R. Mahy, D. Willis, J. Ott, and B. Rosen, *Change Process for the Session Initiation Protocol (SIP)*, RFC 3427, December 2002, ID00 ID01 ID02 ID03
- Fishman, G., and S. Bradner, *Internet Engineering Task Force and International Telecommunication Union - Telecommunications Standardization Sector Collaboration Guidelines*, RFC 3356, August 2002, ID00 ID01ID02
- Bradner, S. Ed. *Intellectual Property Rights in IETF Technology*, Internet Draft, June 2002 (published as RFC 3668) ID01
- Bradner, S. Ed., *IETF Rights in Submissions*, Internet Draft (published as RFC 3667), ID01
- Hoffman, P., and S. Bradner, *Defining the IETF*, RFC 3233, February 2002
- Bradner, S., P. Calhoun, H. Cuschieri, S. Dennett, G. Flynn, M. Lipford, and M. McPheters, *3GPP2-IETF Standardization Collaboration*, RFC 3131, June 2001 ID00
- Bradner, S. and HT Kung, *Requirements for an Anonymizing Packet Forwarder*, Internet Draft, November 2001
- Kung, HT & S. Bradner, *A Framework for an Anonymizing Packet Forwarder*, Internet Draft, November 2001

- Bradner, S. and A. Mankin, *Report of the Next Steps in Signaling BOF*, Internet Draft, July 2001
- Rosenbrock, K., R. Sanmugam, S. Bradner, J. Klensin, *3GPP-IETF Standardization Collaboration*, RFC 3113, June 2001, ID00 ID01
- Gaynor, M. and S. Bradner, *Firewall Enhancement Protocol (FEP)*, RFC 3093, 1-April-2001
- Bradner, S., A. Mankin and J. Schiller, A Framework for Purpose Built Keys (PBK), Internet Draft, February 2001, ID01, ID02, ID03 ID04, ID05
- Bradner, S., A. Mankin and V. Paxson *Advancement of metrics specifications on the IETF Standards Track*, Internet Draft, February 2000, ID01 ID02 ID03
- Bradner, S. and V. Paxson, *IANA Allocation Guidelines For Values In the Internet Protocol and Related Headers*, RFC 2780, March 2000 ID00 ID01 ID02 ID03 ID04
- Bradner, S., *A Memorandum of Understanding for an ICANN Protocol Support Organization*, RFC 2691, September 1999, ID01
- Bradner, S., *A Proposal for an MOU-Based ICANN Protocol Support Organization*, RFC 2690, September 1999, ID00
- Bradner, S., *OSI connectionless transport services on top of UDP Applicability Statement for Historic Status*, RFC 2556, March 1999 ID00 ID01
- Bradner, S., *The Roman Standards Process -- Revision III*, RFC 2551, 1-April-1999
- Bradner, S., and J. McQuaid (Eds.), *Methodology for testing network interconnection devices*, RFC 2544, March 1999
- Bradner, S., *Bylaws for a Protocol Support Organization*, Internet Draft, September 1998, ID01 ID02 ID03
- O'Dell, M., H. Alvestrand, B. Wijnen, and S. Bradner, *Advancement of MIB specifications on the IETF Standards Track*, RFC 2438, October 1998, ID00 ID01
- Bradner, S. *Secret Handshakes: How to get RFCs published in the IETF*, Internet Draft, October 1998 ID01 ID02 ID03
- Brett, R., S. Bradner, and G. Parsons, *Collaboration between ISOC/IETF and ITU-T*, RFC 2436, October 1998
- Bradner, S. (Ed), *IETF Working Group Guidelines and Procedures*, RFC 2418, September 1998, ID00 ID01 ID02 ID03
- Mankin, A., A. Romanow, S. Bradner, V. Paxson, *IETF Criteria for Evaluating Reliable Multicast Transport and Application Protocols*, RFC 2357, June 1998
- Mankin, A., F. Baker, B. Braden, S. Bradner, M. O'Dell, A. Romanow, A. Weinrib, L. Zhang, *Resource ReSerVation Protocol (RSVP) -- Version 1 Applicability Statement Some Guidelines on Deployment*, RFC 2208, September 1997

- Bradner, S. Ed., *Internet Protocol Multicast Problem Statement*, Internet Draft, September 1997
- Bradner, S. Ed., *Internet Protocol Quality of Service Problem Statement*, Internet Draft, September 1997
- Elz, R., R. Bush, S. Bradner and M., Patton, *Selection and Operation of Secondary DNS Servers*, RFC 2182, July 1997
- Bradner, S, *Key words for use in RFCs to Indicate Requirement Levels*, RFC 2119, March 1997 ID00 ID01 ID02
- Bradner, S., *Source directed access control on the Internet.*, RFC 2057, November 1996 ID00 ID01
- R. Hovey and S. Bradner, *The Organizations Involved in the IETF Standards Process*, RFC 2028, October 1996, ID00 ID01 ID02
- Bradner, S. (Ed.), *Internet Standards process - revision 3*, RFC 2026, October 1996, ID00 ID01 ID02 ID03 ID04 ID05 ID06
- Bradner, S., and J. McQuaid (Eds.), *Methodology for testing network interconnection devices*, RFC 1944, May 1996, ID00 ID01 ID02
- Halpern, J. and S. Bradner, *RIPv1 Applicability Statement for Historic Status*, RFC 1923, March 1996
- Bradner, S. and A. Mankin, *The recommendation for the IP next generation protocol*, RFC 1752, January 1995, ID00
- Bradner, S. and A. Mankin, *IP: Next Generation (IPng) White Paper Solicitation*, RFC 1550, December 1993
- Bradner, S. (Ed.), *Benchmarking terminology for network interconnection devices*, RFC 1242, July 1991

Talks (some of the talks I've done over the years)

- Internet Governance: A perpetual "threat"- Harvard Kennedy School, Cambridge MA - 2017-08-02
- The Internet: The anti-network, Harvard College, Cambridge MA 2016-11-07
- IANA, Important but not for what they do, NANOG, Dallas TX, 2016-10-17
- sob@harvard 2/14/66 – 7/1/16, Harvard ABCD, 2015-12-11
- Internet Engineering Task Force (IETF), Harvard Kennedy School, Cambridge MA - 2015-11-18
- Changing Concepts of Anonymity, Confidentiality, and Privacy in SBER, (with Dean Gallant), PRIM&R, Boston MA – 2015-11-12
- "It" will be called "The Internet" but … - NANOG on the Road, Cambridge MA - 2015-04-21
- Internet Governance: A perpetual "threat"- Harvard Kennedy School, Cambridge MA - 2015-01-15

- Random Wanderings – Harvard ABCD, Cambridge MA - 2014-12-12
- Mobile Devices in Research: Growing tool, new issues?, PRIM&R, 2014-12-6
- Governance in a Cyber World - Harvard Kennedy School, Cambridge MA - 2014-07-29
- Internet-101 - Harvard Kennedy School, Cambridge MA - 2014-01-14
- This and That, Harvard ABCD, 2013-12-13
- The Internet, once not, but now, of this world? - Harvard Kennedy School, Cambridge MA - 2013-10-16
- That, This and the Other Thing, Harvard ABCD, Cambridge MA -2013-05-05
- 5 Levels Seems Right, Harvard, 2012-12-03
- Unimaginable but True: the regulatory status of the Internet - Harvard Kennedy School, Cambridge MA - 2012-09-12
- Flowing Down from Layer 9 (say goodbye to the Internet?) - Harvard ABCD, Cambridge MA - 2011-12-09
- Protecting Research Data - PRIM&R - 2011-12-01
- Protecting Research Data - Boston College, Boston MA - 2011-10-17
- Witness to the Evolution: IP from has-been to is-all to ?? - IPTCOMM - 2011-08-01
- Data Security also FISMA - Research Compliance Conference - 2011-06-13
- Technical Issues in Data Security - PRIM&R - 2011-04-29
- Internet-101, Internet Law Forum - 2011-04-08
- Change & Opportunity II, Harvard ABCD – 2010-12-03
- The Internet: Its Past, Present, and Possible Futures - ISOC-NE - 2010-10-20
- Challenges of Research Data Security - EDUCAUSE Security 2010-04-14
- Privacy is not a Spectator Sport - Grand Valley State University, Allendale MI - 2010-02-25
- Change & Opportunity – Harvard ABCD – 2009-12-11
- Research Data Protection Policy at Harvard - PRIM&R - 2009-11-15
- Google Knows: Should you care? – Harvard – 2009-03-11
- New Year, New Rules (No Money) – Harvard ABCD – 2008-12-12
- The Past, Present and Future of the Internet - Boston Network Users Group - 2008-12-02
- Technology Security - Mandatory and Unachievable (but Approachable) - MIT - 2008-11-5
- How is the Internet Different? Is "good enough" good enough? - VON Mexico, Mexico City - 2008-02-28
- Work Mutterings Other Mutterings – Harvard ABCD – 2007-11-02
- The Implications of the Unmet Last Goal for the Internet Protocols - Boston Network Users Group - 2007-01-02

- Security & Privacy Rules & Pre Rules – Harvard ABCD – 2006-07-07
- Where is Controversy? - Alcatel - 2006-11-1
- Will the Internet be permitted to grow up? - Wainhouse Research - 2006-07-20
- Internet II: Looking forward from 10 years ago - Joint Techs - 2006-07-17
- Network Neutrality: Federal Non-Legislation - Cornell, Ithaca NY - 2006-06-28
- Owing the Desktop: Is .edu like .com – Cornell, Ithaca NY - 2006-06-28
- Internet Governance: Not Just Dealing with a Uniqueness Requirement - MIT, Cambridge MA - 2006-05-02
- Not Your Father's Internet, and that Hurts - CENIC, Oakland CA - 2006-04-15
- Internet Concepts, History, Regulations & Governance - Harvard Business School, Boston MA - 2006-04-03
- Security Related Musings - Boston University, Boson MA - 2006-03-01
- The Myth of network Neutrality - EDUCAUSE streaming radio - 2006-02-15
- Where-to-Where (was End-to-End) - Cisco, San Jose CA - 2005-12-07
- Electronic Data Security: Designing a Good Data Protection Plan - Human Research Protection Program (HRPP), Boston MA - 2005-12-06
- This Internet Thing - CS50 - Harvard University, Cambridge MA - 2005-10-22
- Where-to-Where (was End-to-End) - Greater Boston Chapter / ACM - October 20 2005
- NGN: Replacement or Evolution? - FCC, Washington DC - 2005-09-12
- Will the Internet be reliably bad enough to preserve PPVPNs? - MPLSCON, New York, NY - 2005-05-17
- Wireless Grids: The current hype or the next Internet? - TTI Vanguard, Chicago IL - 2005-04-12
- IP nets: from the origins to a possible NGN future - Cisco, San Jose CA - 2005-01-11
- Witness to the Evolution - Cisco Networkers, New Orleans LA - 2004-07-15
- How to Kill Worms and Viruses with Policy Pontifications, NANOG, Miami FL - 2004-02-10
- A Short History of the Internet - NANOG, Miami FL - 2004-02-09
- The Internet Engineering Task Force (IETF) Stuff - Harvard Berkman Center, Cambridge MA - 2003-07-29
- IETF - Global Standards Collaboration 8, Ottawa, Canada - 2003-05-28
- The Internet: Imagination, Innovation or Imitation - USTA - 2003-05-20
- Will the future Internet look like what we have today? - Orange Country IEEE, Irvine CA - 2003-05-20

- Will there be an Internet in 5 years? - Syracuse University, Syracuse NY - 2003-05-08
- Locating the IETF: GIS related work at the IETF - OGC - 2003-02-13
- The Sub-IP Area and Optical Networking at the IETF - GRID Forum, Amsterdam - 2002-09-25
- Internet Architectural Philosophy and the New Business Reality - GRID Forum, Amsterdam - 2002-09-24
- Are technology standards too important to leave to those that know what they are doing? - Public Design Workshop - 2002-09-14
- The IETF: A Decentralized Voluntary Standards Process - SES, Washington DC - 2002-08-13
- The Internet and Optical Networking at the IETF - COIN 2002 - 2002-07-22
- The Future of the Net - Wireless 2002, Calgary AB - 2002-07-08
- Can the e2e RG be real-world useful? - IRTF e2e RG meeting - 2002-05-15
- An IETF Insider View - TranSwitch - 2002-04-15
- The Internet: Philosophy & Technology - Boston University, Boston MA - 2002-02-04
- IETF Stuff, USVP, Mountain View CA, 2002-01-15
- Once there was a network and it was not the one we needed, but the one we built hurts or how the Internet is not the phone network and why that matters to users, service providers, cops and society - MIT, Cambridge MA - 2002-01-10
- The Future of the Net - CINA - 2001-09-15
- Impact of enum and IP telephony - Taiwan - 2001-08-21
- Standards-Setting and United States Competitiveness, Hearing, US. House of Representatives, Committee on Science, Subcommittee on Environment, Technology, and Standards, Washington DC - 2001-06-28
- The future of the nets or will it be The Net? - New England telecommunications Association - 2001-01-17
- Convergence in Telecom Networks: Is there A future? - Lucerne - 2000-11-13
- Convergence Efforts in the IETF - SPIE, Boston MA - 2000-11-08
- Current IETF Efforts and Technology Trends - Lucent - 2000-08-18
- Internet of the Future: Convergence Nirvana? - Broad Band Year, San Jose CA - 2000-06-28
- Internet Engineering Task Force: Standards & ideas for the Internet - G8 meeting, Paris - 2000-05-16
- Internet Engineering Task Force - IPR Summit, London - 2000-04-11

- Next Generation Internet: Where will it stop? - Ericsson, Stockholm - 2000-01-31
- The IETF and the Future of the Internet - ISOC SE, Stockholm - 2000-01-31
- Voice-Over-IP Standards and Interoperability Update IETF - NCF Chicago IL - 1999-10-27
- Does reality matter?: QoS & ISPs – GTE, Burlington MA - 1999-09-15
- WAN Quality of Service - Information Technology Business Forum, Seattle WA - 1999-07-21
- Emerging Trends for the Millennium: Communications Technology - NACAS- 1999-06-26
- The Internet's Impact on Government Programs and Services - Kentucky GIS - 1999-05-03
- Convergence and the IETF - Signaling Futures '99, Tucson AZ - 1999-03-30
- The IETF: Standards and non-Standards - IEEE, Austin TX - 1999-03-08
- Internet Governance: Where are we Now? - Harvard JFK School, Cambridge MA- 1999-02-24
- Technical and Political Issues With Alternatives to Undersea Cables - Nortel - 1998-04-21
- Internet QoS: A definable goal?, Nortel, 1998-04-21
- Real QoS versus a Few Traffic Classes - Next Generation Networks, Washington DC - 1998-11-04
- Internet 2, NGI, and the Real World – Harvard, Cambridge MA - 1998-04-15
- Reality and the Internet of the Future Programs - IEEE - 1998-04-09
- Measuring the Impact of the Integrated Infrastructure for Voice Video and Data on Traditional Telephone Service Administration - IIR, Washington DC - 1998-04-20
- Institutionalizing the IANA Functions To Deliver a Stable and Accessible Global Internet for Mission Critical Business Traffic and Transactions - Reengineering the Internet - London - 1998-01-28
- The problems in trying to create a QoS Internet, ISOC-IL, 1998-01
- Technical and political issues with alternatives to undersea cables, ISOC-IL, 1998-01
- Technology Trends and the IETF - Bellcore - 1997-11-24
- Managing the Bandwidth Explosion - SaskTel, Saskatoon SK - 1997-09-23
- Next Generation Routers - Third Workshop on Real-time and Media Systems (RAMS'97), Taiwan - 1997-08
- Next Generation Routers Overview - Interop - 1997
- Trends and Issues in the next Generation Internet Protocols - Harvard ABCD, Cambridge MA- 1997-07-11

- Reality and the "next generation" projects: NGI, Internet 2 and the real world - U Texas, Austin TX - 1997-04-30
- The future of the Internet - GTE - 1997-04-14
- Internet II Status – IEPG, Memphis TN - 1997-04-06
- IVD at Citicorp - Citicorp, New York City NY - 1997-01-14
- Current Status, Problems and Future Directions of ATM Technology - High Speed Nets - 1996-11
- Under Construction: The Network of the Future - Federal Deposit Insurance Corporation - 1996-11
- Internet II: Introduction – Chicago IL - 1996-10-01
- In whose domain: name service in adolescence (with Don Mitchell & K Claffy) - Harvard JFK School, Cambridge MA - 1996-09-08
- Working Group Workshop – IETF, Los Angeles CA - 1996-03
- Will there be an Internet in the Year 2000? - ATM year, San Jose CA - 1996-05
- The Future of IP - 1996-05-18
- IP Next Generation (IPng), Reseau Interordinateurs Scientifique Quebecois (RISQ) '95, Montreal QU, 1995-01-17
- The new Internet, Reseau Interordinateurs Scientifique Quebecois (RISQ) '95, Montreal QU, 1995-01-17
- Did we miss the fork in the road? - Information Superhighway Summit, San Jose CA - 1994-09-27
- Tunneling - SHARE 83, Boston MA - 1994-08-09
- Internet Engineering Task Force - SHARE 83, Boston MA - 1994-08
- The TCP/IP Protocols - SHARE 83, Boston MA - 1994-08
- Router Tests V.6 - Interop, San Francisco CA - 1993-08-25
- Performance of Routers, Enterprise Networks, Boulder CO - June 15, 1993
- Concept of Routing in a Heterogeneous Network, SHARE 80, San Francisco CA - 1993-04-03
- Routing in IP, SHARE 80, San Francisco CA - 1993-04-03
- Router & Bridge Performance, SHARE 80, San Francisco CA - 1993-04-03
- Network Security, SHARE 80, San Francisco CA - 1993-04-02
- Connecting to the Internet, SHARE 80, San Francisco CA - 1993-04-01
- The AppleTalk & IPX Protocols, SHARE 80, San Francisco CA - 1993-04-01
- Jargon Busting - An Introduction to the Technology of Data Networks, ACM SIGUCCS User Services Conference XX, 1992-11-08
- Kerberos, A User and Service Authentication System, SHARE 79, Atlanta GA, 1992-08-20
- Router & Bridge Performance, SHARE 79, Atlanta GA, 1992-08-19

- Unix Security, SHARE 78, Anaheim CA - 1992-04-04
- Routers versus Bridges, SHARE 78, Anaheim CA - 1992-04-03
- Routers and Bridges Performance, SHARE 78, Anaheim CA - 1992-04-03
- Router Tests V.5 - Interop, Washington DC - 1992-05-20
- NEARnet & NSFnet (& MERIT) (& ANS) - IETF, San Diego CA - 1992-04-14
- Enterprise-wide Network Design - Networks and Imaging Symposium and Exhibition - 1992-02-19
- Router Tests V.4 - Interop, San Jose CA - 1991-10-09
- A Technical Non-IBM View of networking - IBM, Raleigh NC - 1990-11-28
- Traffic Patterns in an X Window Environment - Interop, San Jose CA - 1990-10-11
- Router Tests V.3 – Interop, San Jose CA - 1990-10
- Application of Bridges and Routers - CANET - 1990-06-14
- Worms, Viruses, etc: Things That Go Bump on the Net - SHARE 73, Orlando FL, 1989-08
- Unknown Mailer Error 101, or Why It's So Hard to See You - USENIX, Salt Lake City UT - 1984-06-15
- MLE (Multi-Lingual Editor) - USENIX - 1984-01-18

Last updated: August 19, 2017

LIST OF CASES

Patent litigation in which I was announced as an expert.

Sprint v. Time Warner Cable: USDC Kansas, Case No. 2:11-cv-2686 Kansas, expert for TWC, Jan 2017 to March 2017: Winston & Strawn

OpenTV v. Apple: USDC Northern California Case No. 5:15-cv-02008-EJD, 2016 WL 344845; expert for Apple, June 2015 to Aug 4 2016, declaration: O'Melveny & Meyers (N.D. Cal., dismissed by stipulated order Aug. 4, 2016)

Sprint v Cable One et al: USDC Kansas, Case Nos. 11-2684-JWL, 11-2685-JWL & 11-2686-JWL: expert for Comcast, October 2014 to December 2017, expert report: Winston & Strawn

Sprint v Comcast: Case No. l:12-cv-01013-RGA (D. Del.): expert for Comcast: June 2014 to Jan 2015, expert reports, deposition: Winston & Strawn

Sprint v Big River Telecom: USDC Kansas, Case No. 08-cv-02046-JWL-DJW: expert for Big River Telecom: July 2009 to Sept 2009, expert report: Kirkland & Ellis, (D. Kan., dismissed with prejudice by joint stipulation pursuant to F. R. Civ. P. 41(a)(1)(A)(ii) Sep. 30, 2009)

VoxPath v Verizon: USDC E. TX, Grayson Case No. 4:08-cv-127-RA: expert for Verizon: Dec 2008 to mid 2013: Winston & Strawn (case dismissed with prejudice)

Level3 v. Limelight: USDC E. VA C.A. 2:07CV589 (RGD-FBS): expert for Level 3: Jan 2008 to Jan 2009: expert report, deposition, testified at trial: Winston & Strawn

Verizon v. Vonage: USDC E. VA. CF 1:06CV682 (CMH/BRP): expert for Vonage: Aug 2006 to spring 2007: expert report, deposition: Steptoe & Johnson

Fenner Investments v. Juniper Networks: USDC E. TX. C.A. 2:05CV0: expert for Nortel: April 2006 to mid 2006, expert report: Finnegan, Henderson, Farabow, Garrett & Dunner

Nortel Networks v. Foundry Networks: USDC MA C.A. No. 01-10442DPW: expert for Foundry: October 2002 to October 2004, expert report, deposition: Orrick, Herrington & Sutcliffe

Red River Fiber-Optics Company v. Level 3 Communications: USDC E. TX, Marshall C.A. No. 2-01CV208-TJW: expert for Level 3: October 2002 thru July 2003: expert report, deposition: Merchant Gould

MuniAuction v. Thomson Corporation: expert for Thomson: USDC W. PA C. A. No. 01-1003: June 2002 to Oct 2006: expert report, deposition, testified at trial: Wilmer Cutler Pickering Hale and Dorr

Storage Technology Corporation vs. Cisco Systems: USDC N. CA, San Francisco C.A No. C00-1176 (SI): expert for Storage Technology: December 2000 to June 2005: expert report, deposition, testified at trial: Brooks & Kushman

DataRace vs. Lucent Technologies: expert for Data Race, (Texas): No. CIV.A. SA98CA746PMA: November 1997 to September 1999: expert report, deposition, testified at Markman: McCamish & Socks

In addition, there are a number of cases where I have not yet been announced, that concluded before I was announced or where I served as a consultant.

Inter Parties Reviews in which I provided a declaration.

NFL Enterprises LLC. v. OpenTV Inc., Inter Parties Review, U.S. Patent No. 6,233,736, Case number IPR2017-02092, Expert for NFL, Aug 2017 to July 2018, declaration: Vinson & Elkins LLP, withdrawn

Apple v. OpenTV Inc., Inter Parties Review, U.S. Patent No. 6,233,736, Case number IPR2016-00992, Expert for Apple, Dec 2015 to Aug 2016, declaration: O'Melveny & Meyers, withdrawn

Sony Mobile Communications Inc. v. SSH Communications Security Oyj, Inter Parties Review, U.S. Patent No. 8,544,079, Case number IPR2015-01869, June 2015 to March 2016, Expert for Sony, declaration: Turner Boyd

Sony Mobile Communications Inc. v. SSH Communications Security Oyj, Inter Parties Review, U.S. Patent No. 9,071,578, Case number IPR2016-01180, March 2016 to December 2016, Expert for Sony, declaration: Turner Boyd

Other cases in which I provided a declaration or expert report.

SNMP Research, Inc., et al v Nortel Networks Inc., et al, Chapter 11 09-10138 (KG), Adv. Proc. No. 11-53454 (KG), expert report, 1 Sept 2016 to November 2017.

Nathan Florence et al v. Mark Shurtleff et al, USDC UTAH Central Division, Case Civil No. 2:05CV00485 DB, expert for Nathan Florence et al, declaration, May to December 2011: SNR Denton US

American Booksellers Foundation for Free Expression et al v. Daniel S. Sullivan as Attorney General of the State of Alaska, USDC Alaska, Case No. 3:10-cv-00193-RRB, expert for the American Booksellers Foundation for Free Expression, declaration, August 2010: SNR Denton US

American Booksellers Foundation for Free Expression et al v. Martha Coakley as Attorney General of the State of the Commonwealth of Massachusetts et al, USDC Massachusetts, Civil Action No.: 1:10-cv-11165, expert for the American Booksellers Foundation for Free Expression, declaration, July 2010: SNR Denton US

ACLU v. Reno/American Library Association v. U.S. Department of Justice, Expert for American Library Association, March 1996 to August 1996, declaration, deposition, testified at Federal Court hearing 1996-03-21, 1996-03-22, Jenner & Block

Last updated: September 16, 2018

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix B

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, *Plaintiff*, v. NATIONAL SECURITY AGENCY / CENTRAL SECURITY SERVICE, *et al.*, *Defendants*.	No. 1:15-cv-00662-TSE

DECLARATION OF SCOTT BRADNER
LIST OF DOCUMENTS PROVIDED BY PLAINTIFF'S COUNSEL

A. Documents Included in the Appendix to the Bradner Declaration

1. Appendices C, D–F, H, K, L–U, X–Z, AA, BB, DD–FF

B. Defendants' Discovery Responses

2. Defendant DOJ's Objections and Responses to Plaintiff's First Set of Interrogatories, dated January 2, 2018

3. Defendant DOJ's Objections and Responses to Plaintiff's First and Second Sets of Requests for Admission, dated January 8, 2018

4. Defendant DOJ's Objections and Responses to Plaintiff's First and Second Sets of Requests for Production, dated January 8, 2018

5. Defendant DOJ's January 2018 Production, Bates Numbers DOJ000001-000235 (DOJ Attachments A-C)

6. Defendant NSA's Objections to Plaintiff's Second Set of Interrogatories, dated March 22, 2018

7. Defendant NSA's Objections to Plaintiff's Third Set of Requests for Admission, dated March 22, 2018

8. Defendant NSA's Objections and Responses to Plaintiff's First and Second Sets of Requests for Production, dated January 8, 2018

9. Defendant NSA's January 2018 Production, Bates Numbers NSA-WIKI00000-00297

10. Defendant ODNI's Objections and Responses to Plaintiff's First Set of Interrogatories, dated December 22, 2017

11. Defendant ODNI's Objections and Responses to Plaintiff's First and Second Sets of Requests for Admission, dated January 8, 2018

12. Defendant ODNI's Revised Objections and Responses to Plaintiff's First and Second Sets of Requests for Production, dated February 5, 2018

C. Wikimedia's Discovery Responses

13. Plaintiff Wikimedia Foundation's Responses and Objections to DOJ's First Set of Requests for Production, dated January 26, 2018

14. Plaintiff Wikimedia Foundation's Responses and Objections to NSA's First Set of Requests for Production, dated January 11, 2018

15. Plaintiff Wikimedia Foundation's Responses and Objections to ODNI's Second Set of Interrogatories, dated January 26, 2018

D. Documents Publicly Released by Defendants in *ACLU v. NSA*, 16-cv-8936-RMB (S.D.N.Y.)

16. Bates Numbers ACLU 16-CV-8936 (RMB) 00001-000011: FISC Submission, "2015 Summary of Notable Section 702 Requirements" (July 15, 2015)

17. Bates Numbers ACLU 16-CV-8936 (RMB) 000012-000015: FISC Opinion and Order, *In Re Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search Conducted Under the Foreign Intelligence Surveillance Act* (Aug. 11, 2014)

18. Bates Numbers ACLU 16-CV-8936 (RMB) 000016-000025: FISC Submission, "Government's Response to the Court's Order of July 7, 2015" (July 14, 2015)

19. Bates Numbers ACLU 16-CV-8936 (RMB) 000026-000036: FISC Order, "Order Appointing an Amicus Curiae" (Aug. 13, 2015)

20. Bates Numbers ACLU 16-CV-8936 (RMB) 000037-000038: FISC Submission, "Notice Concerning the Court's Order of August 13, 2015, Appointing an Amicus Curiae" (Aug. 18, 2015)

21. Bates Numbers ACLU 16-CV-8936 (RMB) 000039-000042: FISC Order, "Briefing Order" (Sept. 16, 2015)

22. Bates Numbers ACLU 16-CV-8936 (RMB) 000043-000048: Letter from FBI to FISC Attaching "Annual Report Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act" (Oct. 20, 2014)

23. Bates Numbers ACLU 16-CV-8936 (RMB) 000049-000082: FISC Submission, "Brief of Amicus Curiae" (Oct. 16, 2015)

24. Bates Numbers ACLU 16-CV-8936 (RMB) 000083-000121: FISC Submission, Government's Response to the Court's Briefing Order of September 16, 2015 (Oct. 16, 2015)

25. Bates Numbers ACLU 16-CV-8936 (RMB) 000122-000169: Transcript of FISC Proceedings Held Before the Honorable Thomas F. Hogan (Oct. 20, 2015)

26. Bates Numbers ACLU 16-CV-8936 (RMB) 000170-000177: FISC Submission, "Government's Ex Parte Submission of Attorney General Guidelines" (Aug. 19, 2008)

27. Bates Number ACLU 16-CV-8936 (RMB) 000178: NSA External Oversight Process Description: "Emergency USP Content Queries within FAA 702 PRISM and Telephony Content Collection"

28. Bates Numbers ACLU 16-CV-8936 (RMB) 000179-000183: NSA External Oversight Process Description: "USP Queries within FAA 702 PRISM and Telephone Content Collection"

29. Bates Numbers ACLU 16-CV-8936 (RMB) 000184-000185: DOJ National Security Division Memorandum from Stuart J. Evans, Deputy Assistant Attorney General for Intelligence, to Litigation Section, Office of Intelligence, Re: "Restriction Regarding the Use of FISA Section 702 Information in Criminal Proceedings Against United States Persons"

30. Bates Numbers ACLU 16-CV-8936 (RMB) 000186-000187: NSA External Oversight Process Description: "USP Queries of Communications Metadata Derived from FAA 702 [*Redacted*] and Telephony Collection"

31. Bates Numbers ACLU 16-CV-8936 (RMB) 000188-000190: "USP Query Guidance for Personnel with Access to Unminimized FISA Section 702 Data"

32. Bates Numbers ACLU 16-CV-8936 (RMB) 000191-000221: FISC Submission, "Government's Ex Parte Submission of Reauthorization Certifications and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certifications and Amended Certifications," *In RE DNI/AG 702(g) Certifications* [*Redacted*] (filed Sept. 26, 2016)

33. Bates Numbers ACLU 16-CV-8936 (RMB) 000222-000233: Redacted FISC Submission

34. Bates Numbers ACLU 16-CV-8936 (RMB) 000234-000239: FISC Submission, "Certification of the Director of National Intelligence and the

Attorney General Pursuant to Subsection 702(g) of the Foreign Intelligence Surveillance Act of 1978, As Amended," *In RE DNI/AG 702(g) Certification* [*Redacted*] (filed Sept. 26, 2016)

35. Bates Numbers ACLU 16-CV-8936 (RMB) 000240-000244: FISC Submission, "Affidavit of Admiral Michael S. Rogers, United States Navy, Director, National Security Agency," *In RE DNI/AG 702(g) Certification* [*Redacted*] (filed Sept. 26, 2016)

36. Bates Numbers ACLU 16-CV-8936 (RMB) 000245-000247: FISC Submission, "Affidavit of James B. Comey, Director, Federal Bureau of Investigation," *In RE DNI/AG 702(g) Certification* [*Redacted*] (filed Sept. 26, 2016)

37. Bates Numbers ACLU 16-CV-8936 (RMB) 000248-000250: FISC Submission, "Affidavit of the Director of the Central Intelligence Agency," *In RE DNI/AG 702(g) Certification* [*Redacted*] (filed Sept. 26, 2016)

38. Bates Numbers ACLU 16-CV-8936 (RMB) 000251-000253: FISC Submission, "Affidavit of the Director of the National Counterterrorism Center," *In RE DNI/AG 702(g) Certification* [*Redacted*] (filed Sept. 26, 2016)

39. Bates Numbers ACLU 16-CV-8936 (RMB) 000254-000263: FISC Submission, "Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended" (filed Sept. 26, 2016)

40. Bates Numbers ACLU 16-CV-8936 (RMB) 000264-000280: FISC Submission, "Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended" (filed Sept. 26, 2016)

41. Bates Numbers ACLU 16-CV-8936 (RMB) 000281-000285: FISC Submission, "Procedures Used by the Federal Bureau of Investigation for Targeting Non-United States Persons Reasonably Believed to Be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended" (filed Sept. 26, 2016)

42. Bates Numbers ACLU 16-CV-8936 (RMB) 000286-000328: FISC Submission, "Minimization Procedures Used by the Federal Bureau of Investigation in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended" (signed Sept. 21, 2016)

43. Bates Numbers ACLU 16-CV-8936 (RMB) 000329-000339: FISC Submission, "Minimization Procedures Used by the Central Intelligence Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended" (filed Sept. 26, 2016)

44. Bates Numbers ACLU 16-CV-8936 (RMB) 000340-000343: Redacted FISC Filing, "Exhibit F"

45. Bates Numbers ACLU 16-CV-8936 (RMB) 000344-000358: FISC Submission, "Minimization Procedures Used by the National Counterterrorism Center in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended" (filed Sept. 26, 2016)

46. Bates Numbers ACLU 16-CV-8936 (RMB) 000359-000364: FISC Order, *In RE DNI/AG 702(g) Certifications* [*Redacted*] (Oct. 26, 2016)

47. Bates Numbers ACLU 16-CV-8936 (RMB) 000365-000373: FISC Submission, "Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended" (signed July 24, 2014)

48. Bates Numbers ACLU 16-CV-8936 (RMB) 000374-000419: Transcript of FISC Proceedings Before the Honorable Mary A. McLaughlin, *In RE DNI/AG 702(g) Certification* [*Redacted*] (2008)

49. Bates Numbers ACLU 16-CV-8936 (RMB) 000420-000434: FISC Submission, "Government's Reply to [Redacted] to Petition" (2014)

50. Bates Numbers ACLU 16-CV-8936 (RMB) 000435-000471: Transcript of FISC Proceedings Before the Honorable Thomas F. Hogan (Aug. 4, 2014)

51. Bates Numbers ACLU 16-CV-8936 (RMB) 000472-000509: FISC Submission, "Verified Report in Response to Order," *In RE DNI/AG 702(g) Certification* [*Redacted*] (filed July 18, 2014)

52. Bates Numbers ACLU 16-CV-8936 (RMB) 000510-000548: FISC Opinion (2014)

53. Bates Numbers ACLU 16-CV-8936 (RMB) 000549-000579: FISC Opinion (Apr. 7, 2009)

54. Bates Numbers ACLU 16-CV-8936 (RMB) 000580-000671: FISC Submission, "Quarterly Report to the Foreign Intelligence Surveillance Court

Concerning Compliance Matters Under Section 702 of the Foreign Intelligence Surveillance Act" (Mar. 2015)

55. Bates Numbers ACLU 16-CV-8936 (RMB) 000672-000752: FISC Submission, "Quarterly Report to the Foreign Intelligence Surveillance Court Concerning Compliance Matters Under Section 702 of the Foreign Intelligence Surveillance Act" (Mar. 2014)

56. Bates Numbers ACLU 16-CV-8936 (RMB) 000753-000776: Letter from DOJ National Security Division to FISC Enclosing Memorandum Re: "Discussion with the Foreign Intelligence Surveillance Court on 24 July 2012 Regarding the Waiver Provisions of NSA's Minimization Procedures Governing Data Acquired Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended" (Aug. 28, 2012)

57. Bates Numbers ACLU 16-CV-8936 (RMB) 000792-000841: FISC Submission, "Government's Ex Parte Submission of Reauthorization Certifications and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certifications and Amended Certifications" (filed July 15, 2015)

58. Bates Numbers ACLU 16-CV-8936 (RMB) 000842-000847: FISC Submission, "Certification of the Director of National Intelligence and the Attorney General Pursuant to Subsection 702(g) of the Foreign Intelligence Surveillance Act of 1978, As Amended," *In RE DNI/AG 702(g) Certification* [*Redacted*] (filed July 15, 2015)

59. Bates Numbers ACLU 16-CV-8936 (RMB) 000848-000851: FISC Submission, "Affidavit of Admiral Michael S. Rogers, United States Navy, Director, National Security Agency," *In RE DNI/AG 702(g) Certification* [*Redacted*] (filed July 15, 2015)

60. Bates Numbers ACLU 16-CV-8936 (RMB) 000852-000854: FISC Submission, "Affidavit of James B. Comey, Director, Federal Bureau of Investigation," *In RE DNI/AG 702(g) Certification* [*Redacted*] (filed July 15, 2015)

61. Bates Numbers ACLU 16-CV-8936 (RMB) 000855-000857: FISC Submission, "Affidavit of the Director of the Central Intelligence Agency," *In RE DNI/AG 702(g) Certification* [*Redacted*] (filed July 15, 2015)

62. Bates Numbers ACLU 16-CV-8936 (RMB) 000858-000862: FISC Submission, "Procedures Used by the Federal Bureau of Investigation for Targeting Non-United States Persons Reasonably Believed to Be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended" (filed July 28, 2014)

63. Bates Numbers ACLU 16-CV-8936 (RMB) 000863-000866: Redacted FISC Filing, "Exhibit F"

64. Bates Numbers ACLU 16-CV-8936 (RMB) 000867-000898: FISC Submission, "Government's Verified Response to the Court's Order Dated October 14, 2015" (filed Oct. 21, 2015)

65. Bates Numbers ACLU 16-CV-8936 (RMB) 000899-000910: FISC Submission, "Verified Response to the Court's Order Dated November 6, 2015" (signed Dec. 18, 2015)

66. Bates Numbers ACLU 16-CV-8936 (RMB) 000911-001000: NSA Analysis & Production, "Draft FAA 702 Guidance"

67. Bates Numbers ACLU 16-CV-8936 (RMB) 001001-001049: "FAA 702 Adjudication Checklist"

68. Bates Numbers ACLU 16-CV-8936 (RMB) 001050-001096: "OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL," at 36-82

69. Bates Numbers ACLU 16-CV-8936 (RMB) 001097-001100: "OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL," at 83-86

70. Bates Numbers ACLU 16-CV-8936 (RMB) 001101-001150: NSA Presentations, "FAA 702 Metrics Update" (Dec. 2013-Feb. 2016)

71. Bates Numbers ACLU 16-CV-8936 (RMB) 001151-001189: NSA Presentations, "FAA 702 Metrics Update" (Mar.-Aug. 2016)

72. Bates Numbers ACLU 16-CV-8936 (RMB) 001190-001228: NSA Presentations, "FAA 702 Metrics Update" (Aug.-Dec. 2016)

73. Bates Numbers ACLU 16-CV-8936 (RMB) 001229-001230: NSA Presentations, "FAA 702 Metrics Update" (Dec. 2016)

74. Bates Numbers ACLU 16-CV-8936 (RMB) 001231-001235: NSA, "Report of Annual Review Pursuant to Section 702(I) of the Foreign Intelligence Surveillance Act for Period 9/1/2012 Through 8/31/2013"

75. Bates Numbers ACLU 16-CV-8936 (RMB) 001236-001240: "National Security Agency Response to Congressionally Direction Action: Report of Annual Review Pursuant to Section 702(I) of the Foreign Intelligence Surveillance Act for Period 9/1/2013 Through 8/31/2014"

76. Bates Numbers ACLU 16-CV-8936 (RMB) 001241-001244: "National Security Agency Response to Congressionally Direction Action: Report of

Annual Review Pursuant to Section 702(I) of the Foreign Intelligence Surveillance Act for Period 9/1/2014 Through 8/31/2015"

77. Bates Numbers ACLU 16-CV-8936 (RMB) 001245-001247: "National Security Agency Response to Congressionally Direction Action: Report of Annual Review Pursuant to Section 702(I) of the Foreign Intelligence Surveillance Act for Period 9/1/2015 Through 8/31/2016"

78. Bates Numbers ACLU 702 FOIA 09 15 2017 release 000001-000057: "Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence" (Feb. 2016)

79. Bates Numbers ACLU 702 FOIA 09 15 2017 release 000058-000066: ODNI, "Annual Statistical Transparency Report Regarding Use of National Security Authorities for Calendar Year 2015" (Apr. 30, 2016)

E. Documents Publicly Released by Defendants in *EFF v. DOJ*, 16-cv-02041 (N.D. Cal.), http://icontherecord.tumblr.com/post/161824569523/additional-release-of-fisa-section-702-documents

80. Document 1: FISC Opinion (2008)

81. Document 2: FISC Opinion (2010)

82. Document 3: FISC Opinion and Order (Aug. 30, 2013)

83. Document 4: FISC Opinion and Order (2010)

84. Document 5: FISC Opinion and Order (2009)

85. Document 6: FISC Opinion (2014)

86. Document 7: FISC Opinion and Order (2012)

87. Document 8: FISC Order (Oct. 29, 2013)

88. Document 9: FISC Order Re: DNI/AG 702(g) [Redacted] (2010)

89. Document 10: FISC Order (2009)

90. Document 11: FISC Opinion and Order (2009)

91. Document 12: FISC Opinion on Motion for Disclosure of Prior Decisions (2014)

92. Document 13: FISC Opinion (2010)

93. Document 14: FISC Opinion and Order (Apr. 7, 2009)

94. Document 15: FISC Opinion and Order (Dec. 13, 2013)

95. Document 16: FISC Briefing Order (2010)

96. Document 17: FISC Briefing Order (Oct. 13, 2011)

97. Document 18: FISC Order (Oct. 29, 2013)

F. Documents Publicly Released by Defendants in *N.Y. Times v. DOJ*, 16-cv-07020 (S.D.N.Y.)

98. Bates Numbers NYT v. DOJ, 16 CIV 7020_000041-000049: First Tranche (4 documents totaling 11 pages), *available at:* https://www.documentcloud.org/documents/3867003-Savage-NYT-FOIA-2011-FISC-MCT-Files.html

99. Bates Numbers NYT v. DOJ, 16 CIV 7020_000050-000237: Second Tranche (11 documents totaling 175 pages), *available at:* https://www.documentcloud.org/documents/3986047-Savage-NYT-FOIA-NSA-MCT-Bates-Case-Files.html

100. Bates Numbers NYT v. DOJ, 16 CIV 7020_000411-000585: Third Tranche (12 documents totaling 190 pages), *available at:* https://www.documentcloud.org/documents/4064819-Savage-NYT-FOIA-2011-Bates-MCT-third-tranche.html

G. Other Documents Publicly Released by Defendants

101. FISC Opinion and Order Concerning "Government's Ex Parte Submission of Reauthorization Certifications and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certifications and Amended Certifications" (filed Nov. 6, 2015)

102. FISC Submission, "Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended" (filed July 15, 2015)

103. FISC Opinion and Order Concerning "Government's Ex Parte Submission of Reauthorization Certifications and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certifications and Amended Certifications" (Sept. 20, 2012)

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix C

This document was also filed as ECF No. 168-27 and can be found in this Joint Appendix at JA2890.

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix D

This document was also filed as ECF No. 168-22 and can be found in this Joint Appendix at JA2721.

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix E

This document was also filed as ECF No. 168-25 and can be found in this Joint Appendix at JA2790.

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix F

This document was also filed as ECF No. 168-19 and can be found in this Joint Appendix at JA2434.

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix G

ON DISTRIBUTED COMMUNICATIONS NETWORKS

Paul Baran

September 1962

P-2626

ON DISTRIBUTED COMMUNICATIONS NETWORKS

Paul Baran*

The RAND Corporation, Santa Monica, California

INTRODUCTION

The previous paper** described how redundancy of coding can be used to build efficient digital data links out of transmission links of variable and often less than presently useful quality. An arbitrarily low over-all error rate can be purchased with a modest redundancy of coding and clever terminal equipment. But even links with low error rates can have less than perfect reliability.

We should like to extend the remarks of the previous paper and address ourselves to the problem of building

---

*Any views expressed in this paper are those of the author. They should not be interpreted as reflecting the views of The RAND Corporation or the official opinion or policy of any of its governmental or private research sponsors. Papers are reproduced by The RAND Corporation as a courtesy to members of its staff.

This paper was prepared for presentation at the First Congress of the Information Systems Sciences, sponsored by The MITRE Corporation and the USAF Electronic Systems Division, November, 1962.

The writer is indebted to John Bower for his suggestions that switching in any store-and-forward system can be described by a model of a postmaster at a blackboard. Programming assistance provided by Sharla Boehm, John Derr, and Joseph Smith is gratefully acknowledged.

**A prior paper was presented by Paul Rosen and Irwin Lebow of MIT Lincoln Laboratories, discussing redundancy of coding on a single link, "Low Error Efficient Digitial Communications Links," First Congress on the Information Systems Sciences, McGraw-Hill, New York, 1962.

digital communication networks using links with less than perfect reliability. We shall again trade in the currency of redundancy, but instead of redundancy of coding we shall make use of redundancy of connectivity.

This thing called redundancy is a powerful tool. But the systems planner must choose that form of redundancy so that the form of the "noise" or interference appears to be somewhat statistically independent for each redundant element added. If this goal is completely met, there can be an exponential payoff for a linear increase of added elements. As an example, we shall consider in some detail the synthesis of a system where the form of the disturbance or "noise" is the simultaneous destruction of many geographically separated installations. The system in particular is to be a very high-speed digital data transmission network composed of unreliable links, but which exhibits any arbitrarily desired level of system reliability or survivability.

DEFINITION OF SURVIVABILITY

This communications network shall be composed of several hundred stations which must intercommunicate with one another. Survivability as herein defined is the percentage of stations surviving a physical attack and remaining in electrical connection with the largest single group of surviving stations. This criterion is a measure of the ability of the surviving stations to operate together as a coherent entity after attack.

TYPES OF NETWORKS

Although one can draw a wide variety of networks, they all factor into two components: centralized (or star) and distributed (or grid or mesh). (Types (a) and (c) in Fig. 1)

The centralized network is basically vulnerable. Destruction of the central node destroys intercommunication between the end stations. In practice, a mixture of star and mesh components is used to form communications networks. For example, type (b) in Fig. 1 shows a hierarchial structure to a set of stars connected in the form of a larger star with an additional link forming a loop. Such a network is sometimes called a "decentralized" network, because complete reliance upon a single point is not always required. But, as destruction of a small number of nodes in a decentralized network can destroy communications, we shall turn to consider the properties, problems, and hopes of building communications networks that are as "distributed" as possible. The unstandardized terms centralized, decentralized, and distributed are often and conveniently used as relative adjectives when referring to real-world networks.

DEFINITION OF REDUNDANCY LEVEL

Figure 2 defines the term "redundancy level," which is used in this paper as a measure of connectivity. A minimum span network, one formed with the smallest number

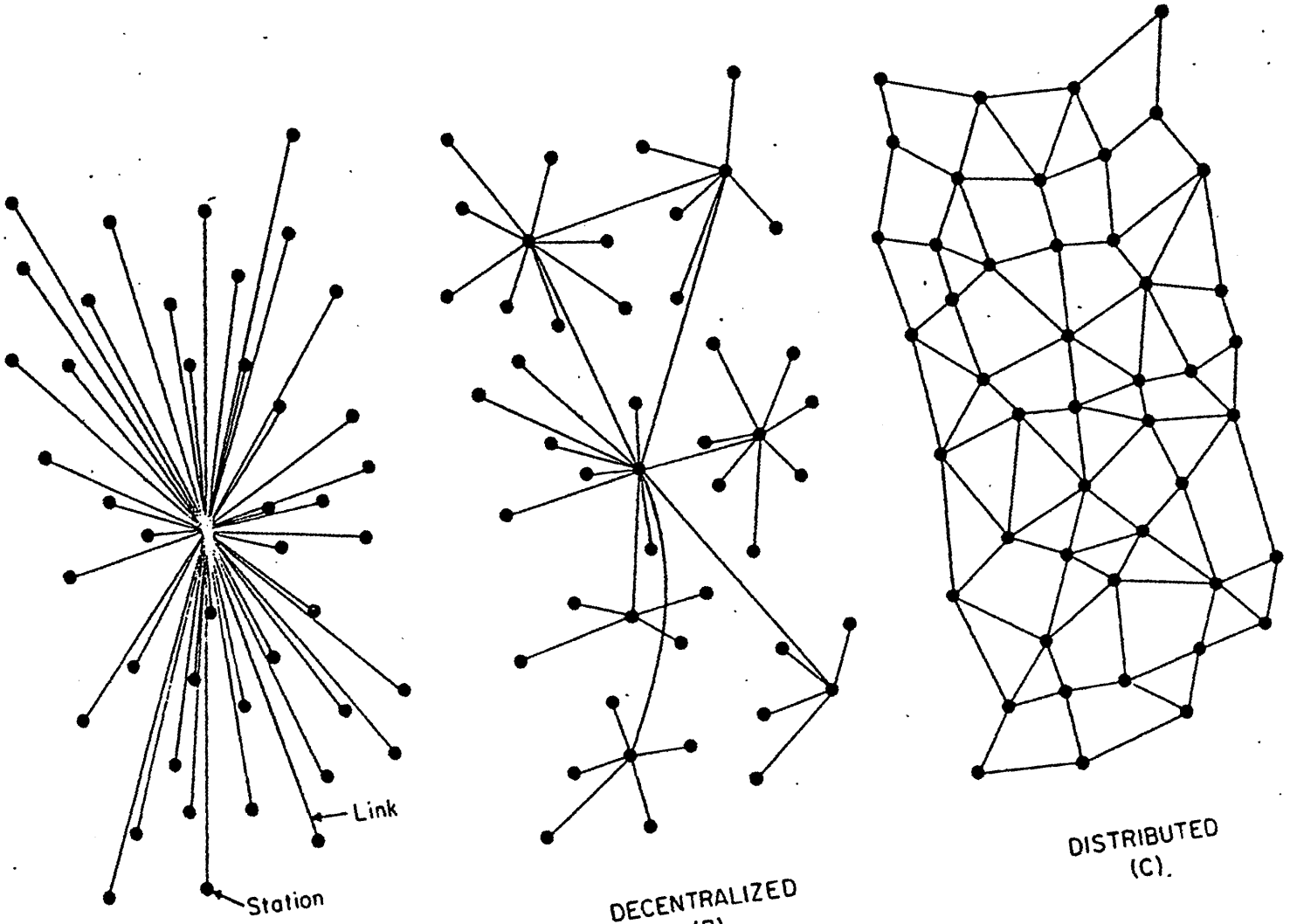


FIG. 1 — Centralized, Decentralized and Distributed Networks

of links possible, is chosen as a reference point, and is called "a network of redundancy level one." If two times as many links are used in a gridded network than in a minimum span network, the network is said to have a redundancy level of two. Figure 2 defines connectivity of 1, 1½, 2, 3, 4, 6, and 8. Redundancy level is equivalent to link-to-node ratio in an infinite size arrays of stations.

ASSUMPTION OF PERFECT SWITCHING

Each node and link in the array of Fig. 2 has the capacity and the switching flexibility to allow transmission between any ith station and any jth station, provided a path can be drawn from the ith to the jth station.

Starting with a network composed of an array of stations connected as in Fig. 3, an assigned percentage of nodes and links are destroyed. If, after this operation, it is still possible to draw a line to connect the ith station to the jth station, the ith and jth stations are said to be connected.

RATIONALE FOR DESTRUCTION PATTERNS

Figure 4 indicates network performance as a function of the probability of destruction for each separate node. If the expected "noise" was destruction caused by conventional hardware failure, the failures would be randomly distributed through the network. But, if the disturbance

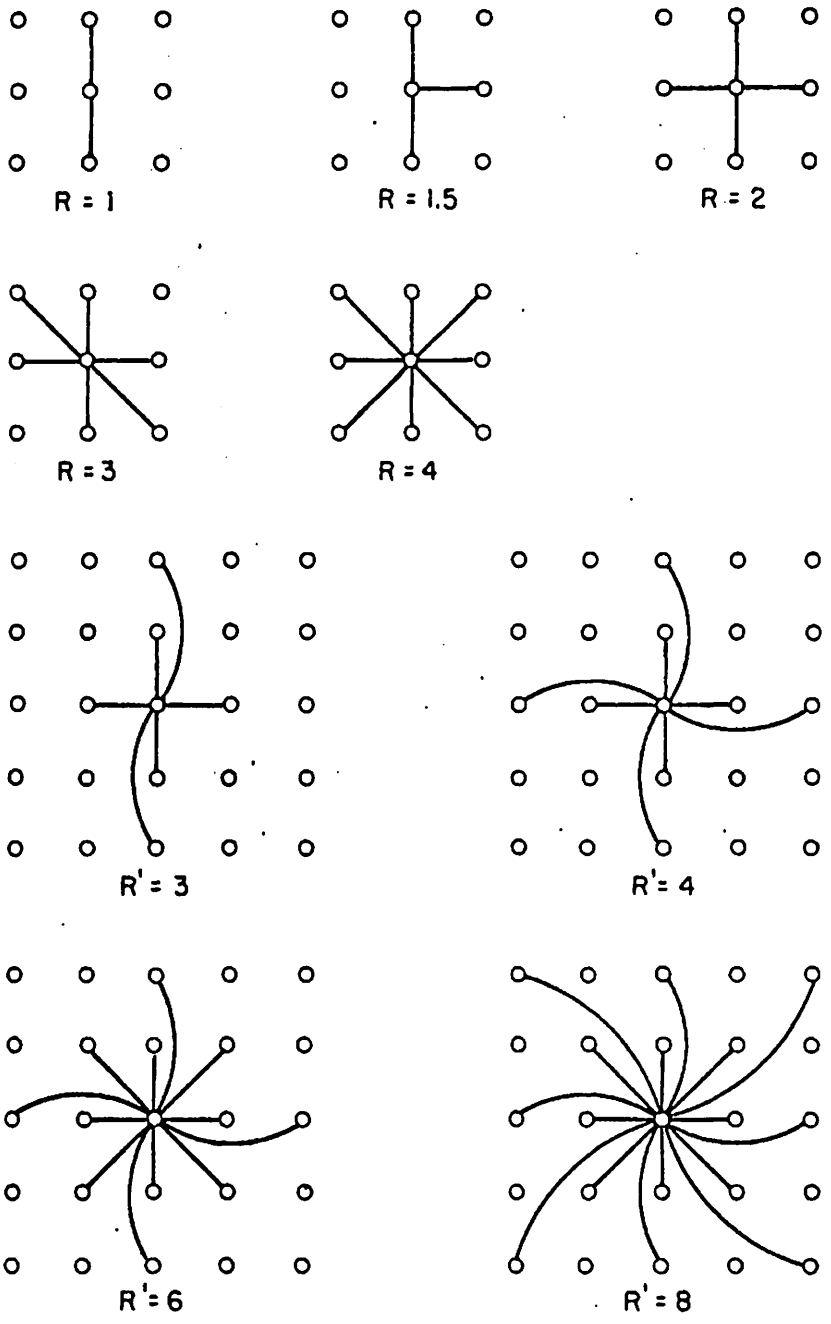


FIG. 2 – Definition of Redundancy Level

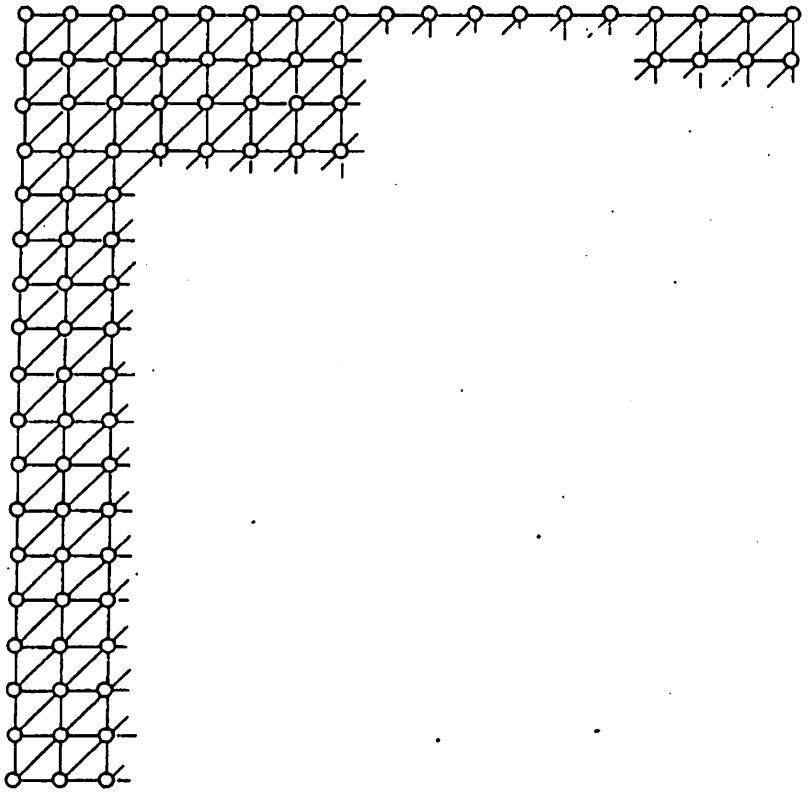


FIG. 3 — An Array of Stations

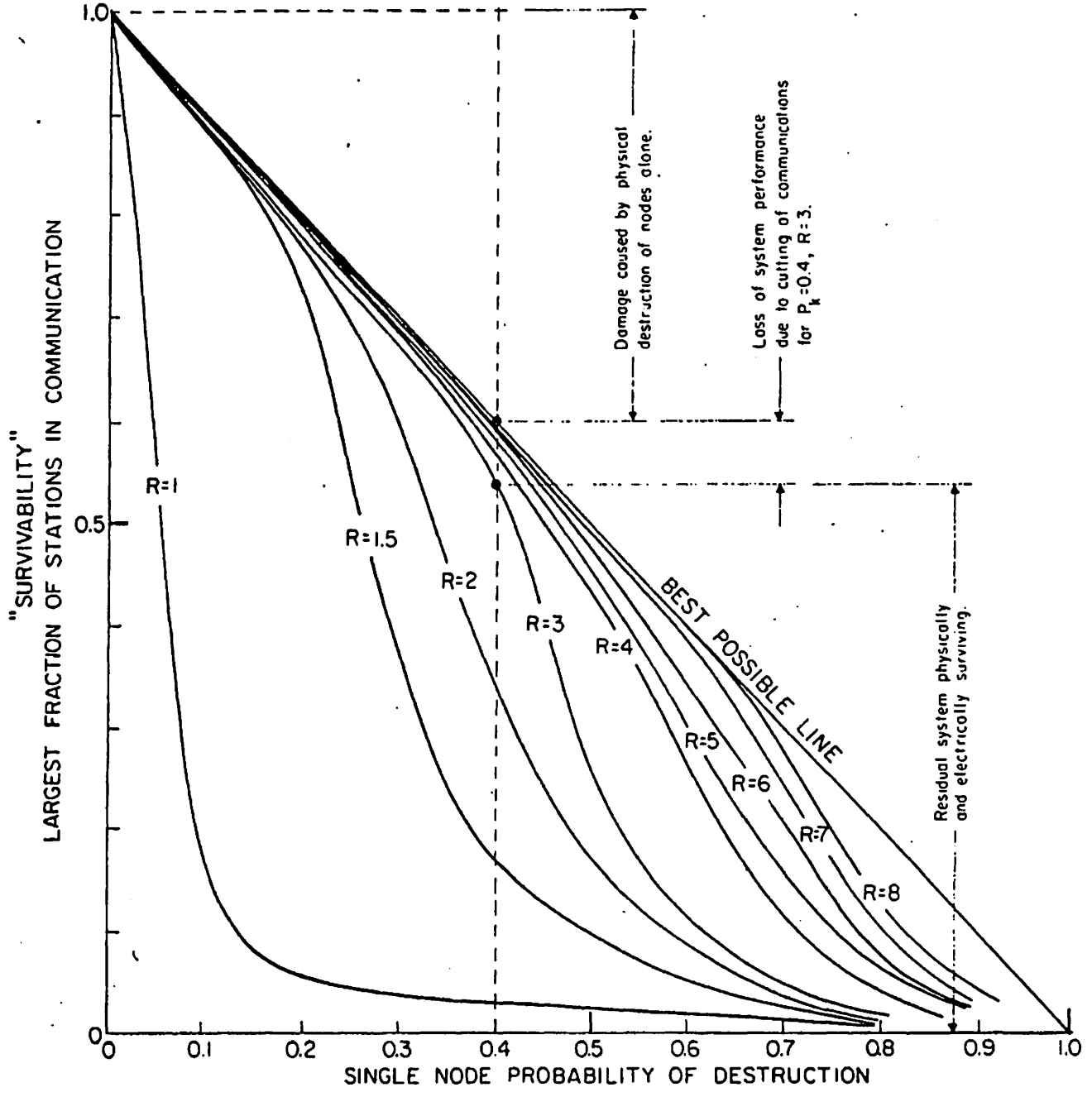


FIG. 4 — Perfect Switching in a Distributed Network — Sensitivity to Node Destruction, 100% of Links Operative.

were caused by enemy attack there are two possible "worst cases" to be considered.

To bisect a 32-link width network requires direction of 288 weapons each with a probability of kill, $p_k = 0.5$, or 160 with a $p_k = 0.7$, to produce over an 0.9 probability of successfully bisecting the network. If hidden alternative command is allowed, then the largest single group would still have an expected value of almost 50 percent of the initial stations surviving intact. If this raid misjudges complete availability of weapons, or complete knowledge of all links in the cross section, or the effects of the weapons against each and every link, the raid fails. The high risk of such raids against highly parallel structures causes examination of alternative attack policies. Consider the following uniform raid example. Assume that 2,000 weapons are deployed against a 1000-station network. The stations are so spaced that destruction of two stations with a single weapon is unlikely. Divide the 2,000 weapons into two equal 1,000 weapon salvos. Assume any probability of destruction of a single node from a single weapon less than 1.0; for example, 0.5. Each weapon on the first salvo has a 0.5 probability of destroying its target. But, each weapon of the second salvo has only a 0.25 probability, since one-half the targets have already been destroyed. Thus, the uniform attack is felt to represent a worst-case configuration.

MONTE CARLO SIMULATION

Such worst-case attacks have been directed against an 18x18-array network model of 324 nodes with varying probability of kill and redundancy level, with results shown in Fig. 4. The probability of kill was varied from zero to unity along the abscissa while the ordinate marks survivability. The criterion of survivability used is the percentage of stations not physically destroyed and remaining in communications with the largest single group of surviving stations. The curves of Fig. 4 demonstrate survivability as function of attack level for networks of varying degrees of redundancy. The line labeled "best possible line" marks the upper bound of loss due to the physical failure component alone. For example, if a network underwent an attack of 0.5 probability destruction of each of its nodes, then only 50 per cent of its nodes would be expected to survive--regardless of how perfect its communications. We are primarily interested in the additional system degradation caused by failure of communications. Two key points are to be noticed in the curves of Fig. 4. First, extremely survivable networks can be built using a moderately low redundancy of connectivity level. Redundancy levels on the order of only three permit withstanding extremely heavy level attacks with negligible additional loss to communications. Secondly, the survivability curves have sharp break-points.

A network of this type will withstand an increasing attack level until a certain point is reached, beyond which the network rapidly deteriorates. Thus, the optimum degree of redundancy can be chosen as a function of the expected level of attack. Further redundancy buys little. The redundancy level required to survive even very heavy attacks is not great--on the order of only three or four times that of the minimum span network.

SIMULATION RESULTS--LINK FAILURE ONLY

In the previous example we have examined network performance as a function of the destruction of the nodes (which are better targets than links). We shall now reexamine the same network, but using unreliable links. In particular, we want to know how unreliable the links may be without further degrading the performance of the network.

Figure 5 shows the results for the case of perfect nodes; only the links fail. There is little system degradation caused even using extremely unreliable links--on the order of 50 percent down-time--assuming all nodes are working.

COMBINATION LINK AND NODE FAILURES

The worst case is the composite effect of failures of both the links and the nodes. Figure 6 shows the effect of link failure upon a network having 40 percent of its nodes destroyed. It appears that what would today be regarded as an unreliable link can be used in a distributed

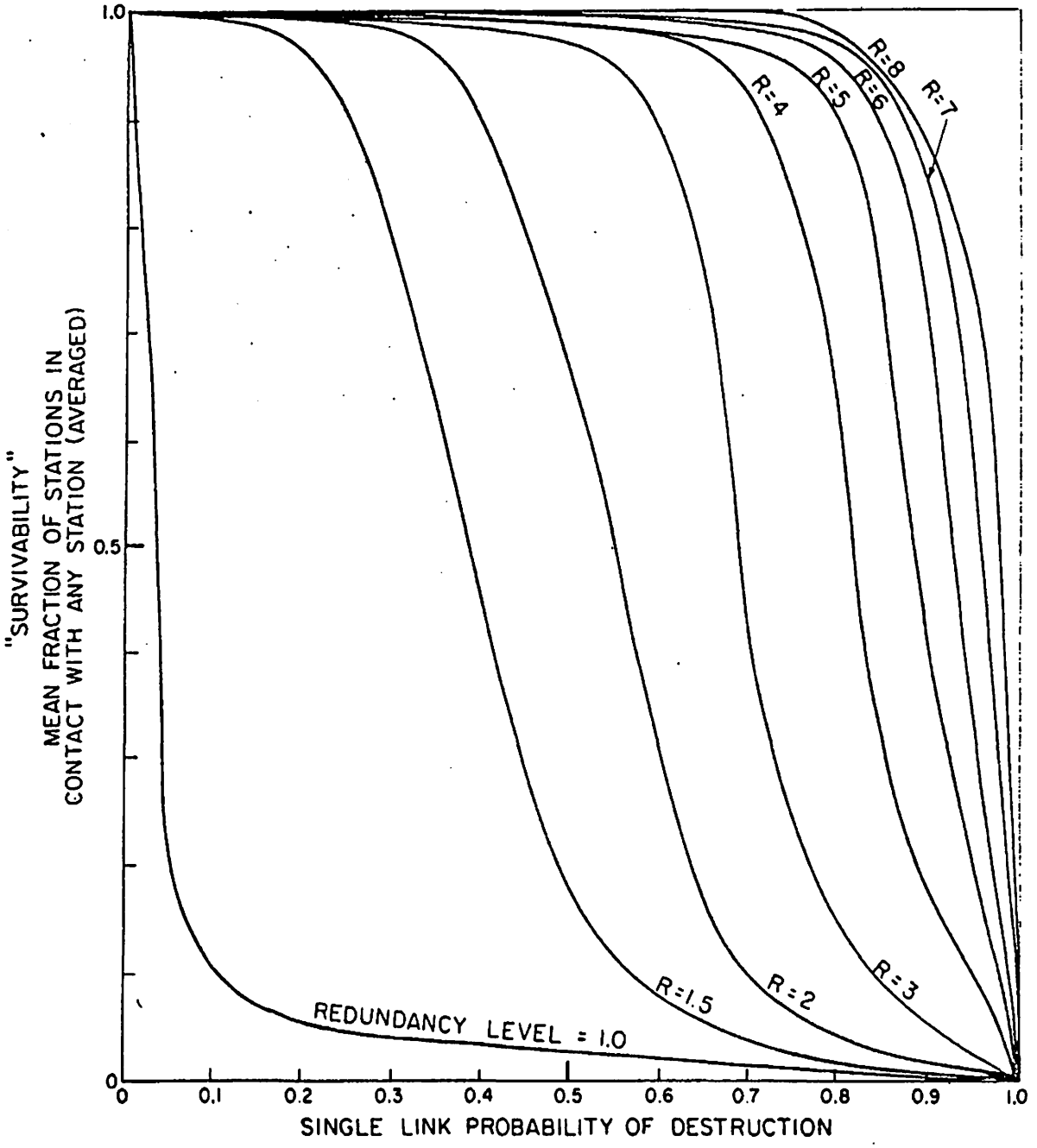


FIG. 5 — Perfect Switching in a Distributed Network — Sensitivity to Link Destruction, 100% of Nodes Operative.

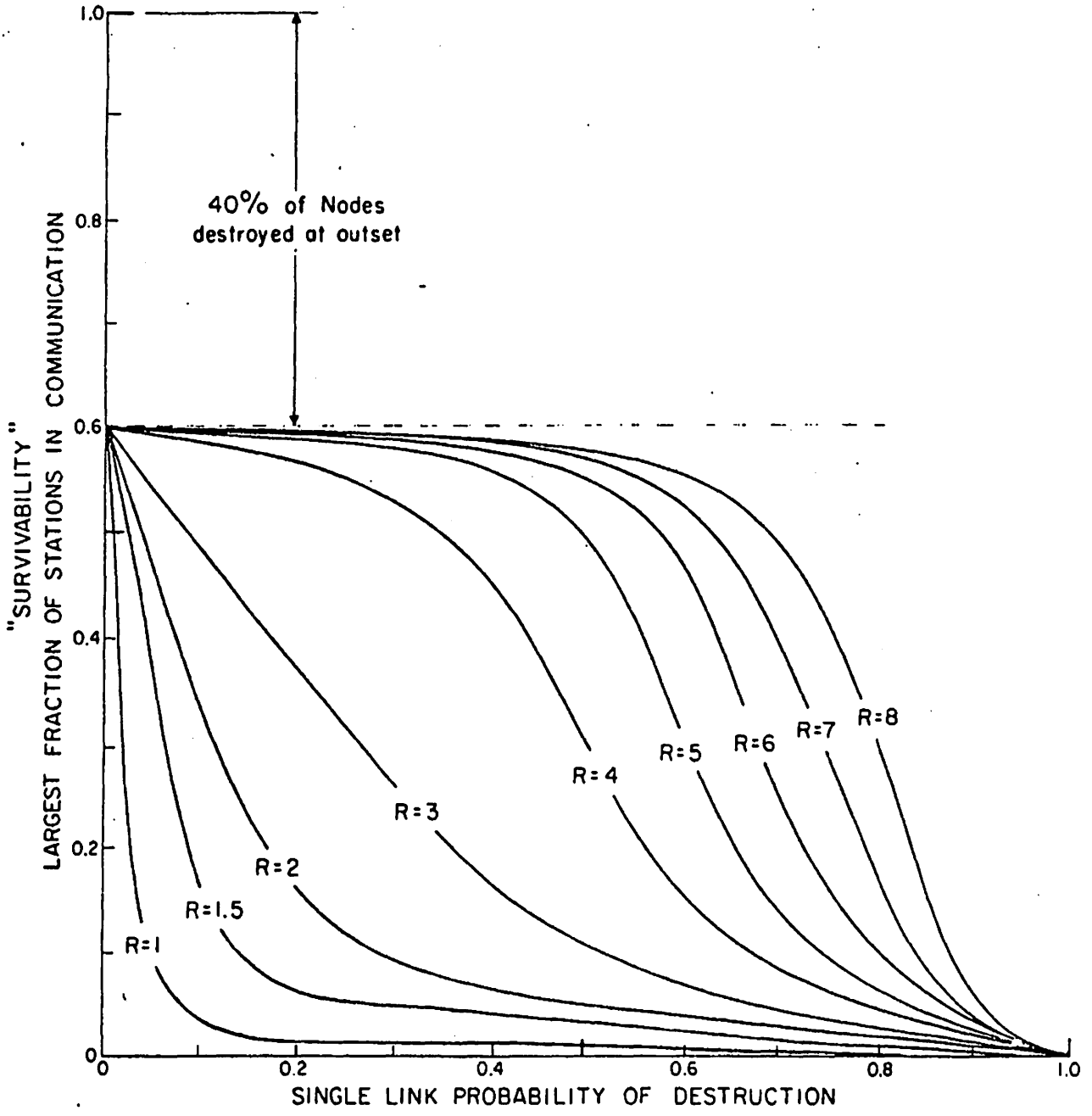


FIG. 6 – Perfect Switching in a Distributed Network — Sensitivity to Link Destruction After 40% Nodes Are Destroyed.

network almost as effectively as perfectly reliable links. Figure 7 examines the result of 100 trial cases in order to estimate the probability density distribution of system performance for a mixture of node and link failures. This is the distribution of cases for 20 percent nodal damage and 35 percent link damage.

DIVERSITY OF ASSIGNMENT

There is another and more common technique for using redundancy than in the method described above in which each station is assumed to have perfect switching ability. This alternative approach is called "diversity of assignment." In diversity of assignment, switching is not required. Instead, a number of independent paths are selected between each pair of stations in a network which requires reliable communications. But, there are marked differences in performance between distributed switching and redundancy of assignment as revealed by the following Monte Carlo simulation.

In the matrix of N separate stations, each ith station is connected to every jth station by three shortest but totally separate independent paths ($i=1,2,3,\ldots,N$; $j=1,2,3,\ldots,N$; $i \neq j$). A raid is laid against the network. Each of the pre-assigned separate paths from the ith station to the jth station is examined. If one or more of the pre-assigned paths survive, communication is said to exist between the ith and the jth station. The criterion of

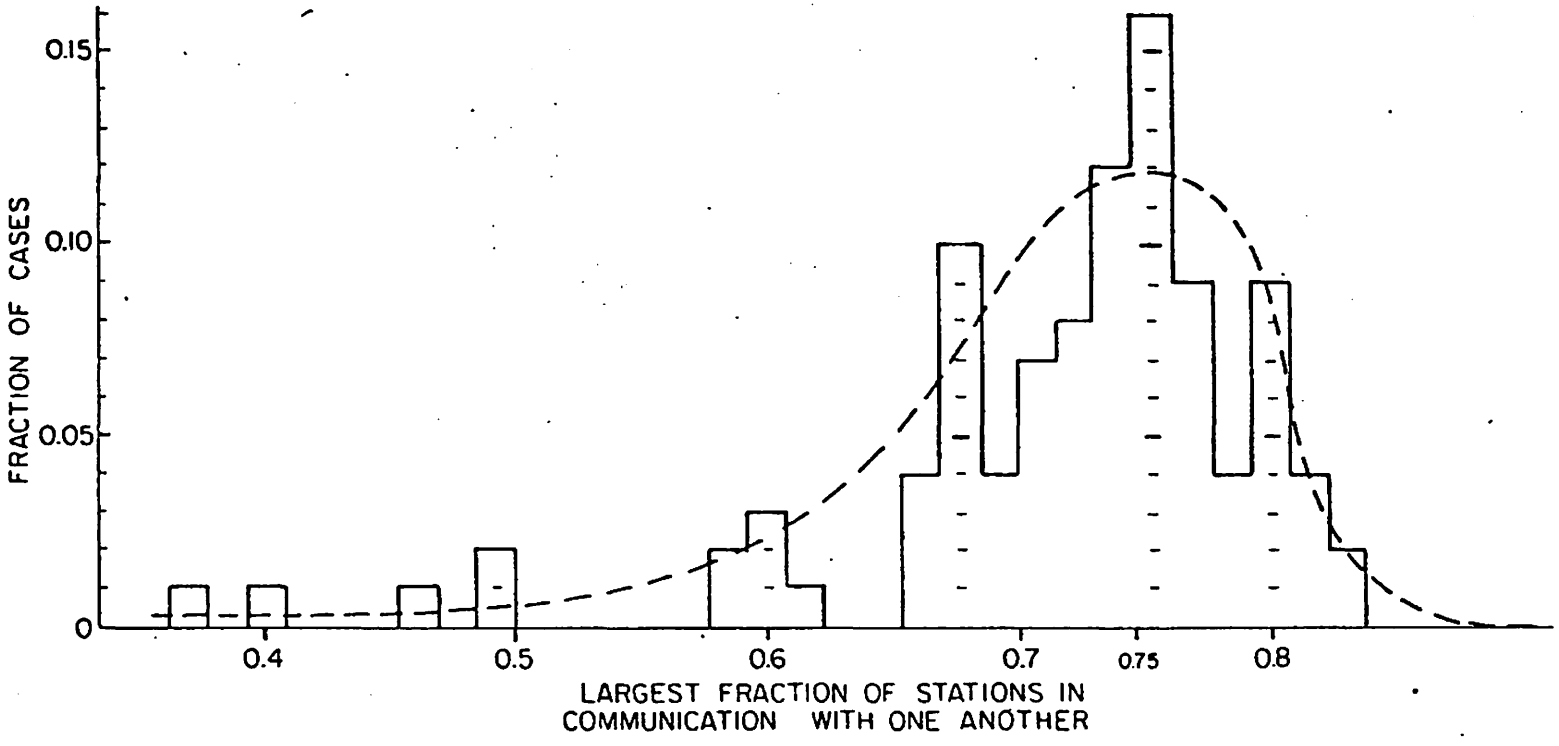


FIG. 7 — Probability Density Distribution of Largest Fraction of Stations in Communication Perfect Switching, R = 3, 100 Cases, 80% Node Survival, 65% Link Survival.

survivability used is the mean number of stations connected to each station, averaged over all stations.

Figure 8 shows, unlike the distributed perfect switching case, that there is a marked loss in communications capability with even slightly unreliable nodes or links. The difference can be visualized by remembering that fully flexible switching permits the communicator the privilege of ex post facto decision of paths. Figure 8 emphasizes a key difference between some present day networks and the fully flexible distributed network we are discussing.

COMPARISON WITH PRESENT SYSTEMS

Present conventional switching systems try only a small subset of the potential paths that can be drawn on a gridded network. The greater the percentage of potential paths tested, the closer one approaches the performance of perfect switching. Thus, perfect switching provides an upper bound of expected system performance for a gridded network; the diversity of assignment case, a lower bound. Between these two limits lie systems composed of a mixture of switched routes and diversity of assignment.

Diversity of assignment is useful for short paths, eliminating the need for switching, but requires survivability and reliability for each tandem element in long haul circuits passing through many nodes. As every component in at least one out of a small number of possible paths

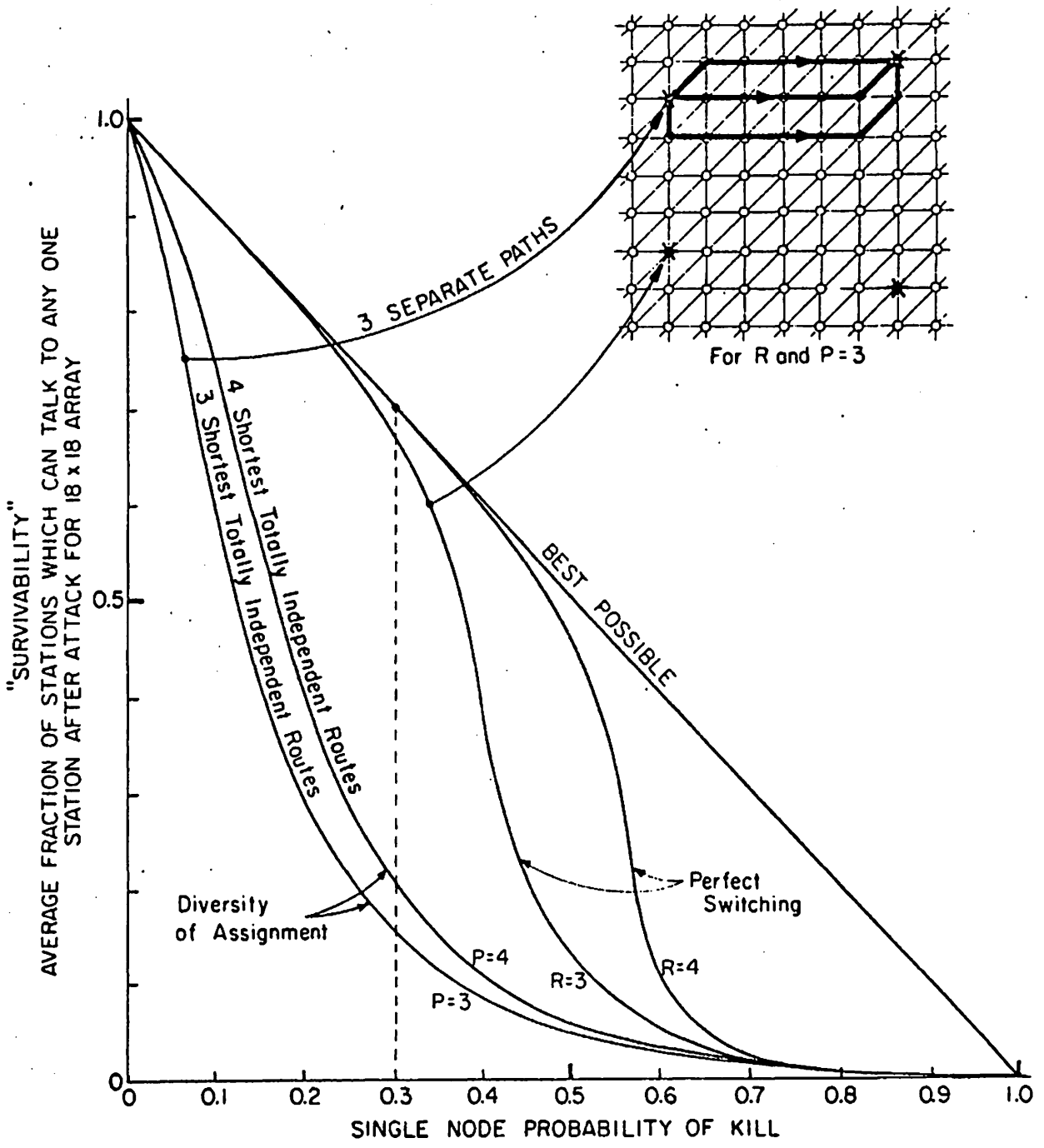


FIG. 8 – Diversity of Assignment vs. Perfect Switching in a Distributed Network.

must be simultaneously operative, high reliability margins and full standby equipment are usual.

ON FUTURE SYSTEMS

We will soon be living in an era in which we cannot guarantee survivability of any single point. However, we can still design systems in which system destruction requires the enemy to pay the price of destroying n of n stations. If n is made sufficiently large, it can be shown that highly survivable system structures can be built--even in the thermonuclear era. In order to build such networks and systems we will have to use a large number of elements. We are interested in knowing how inexpensive these elements may be and still permit the system to operate reliably. There is a strong relationship between element cost and element reliability. To design a system that must anticipate a worst-case destruction of both enemy attack, and normal system failures, one can combine the expected failures expected by enemy attack together with the failures caused by normal reliability problems, provided the enemy does not know which elements are inoperative. Our future systems design problem is that of building very reliable systems out of the described set of unreliable elements at lowest cost. In choosing the communications links of the future, digital links appear increasingly attractive by permitting low cost switching and low cost links. For example, if "perfect

switching" is used, digital links are mandatory to permit tandem connection of many separately connected links without cumulative errors reaching an irreducible magnitude. Further, the signalling measures to implement highly flexible switching doctrines always require digits.

FUTURE LOW COST ALL-DIGITAL COMMUNICATIONS LINKS

When one designs an entire system optimized for digits and high redundancy, certain new communications-link techniques appear more attractive than those common today.

A key attribute of the new media is that it permits formation of new routes cheaply, yet allows transmission on the order of a million or so bits per second, high enough to be economic, but yet low enough to be inexpensively processed with existing digital computer techniques at the relay station nodes. Reliability and raw error rates are secondary. The network must be built with the expectation of heavy damage, anyway. Powerful error removal methods exist.

Some of the communication construction methods that look attractive in the near future include pulse regenerative repeater line, "poor-boy" microwave, TV broadcast station digital transmission, and non-synchronous satellites.

Pulse Regenerative Repeater Line

Samuel B. Morse's regenerative repeater invention for amplifying weak telegraphic signals has recently been

resurrected and transistorized. Morse's electrical relay permits amplification of weak binary telegraphic signals above a fixed threshold. Experiments by various organizations (primarily the Bell Telephone Laboratories) have shown that digital data rates on the order of 1.5 million bits per second can be transmitted over ordinary telephone line at repeater spacings on the order of 6,000 feet for #22 gage pulp paper insulated copper pairs. At present, up to 20 tandemly connected amplifiers have been used without retiming synchronization problems. There appears to be no fundamental reason why either lines of lower loss with corresponding further repeater spacing, or more powerful resynchronization methods cannot be used to extend link distances to in excess of 100 miles. Such distances would be desired for a possible national distributed network.

Power to energize the miniature transistor amplifier is transmitted over the copper circuit itself.

"Poor-Boy" Microwave

While the price of microwave equipment has been declining, there are still untapped major savings. In an analog signal network we require a high degree of reliability and very low distortion for each tandem repeater. However, using digital modulation together with perfect switching we minimize these two expensive considerations from our planning. We would envision the use of almost mass-produced

microwave crystal receiver/klystron oscillator units mounted on "telegraph poles" carrying commercial power. Relay station spacing would probably be on the order of 10+ miles. Further economies can be obtained by only a minimal use of standby equipment and reduction of fading margins. The ability to use alternate paths permits consideration of frequencies normally troubled by rain attenuation problems reducing the spectrum availability problem.

While this technique has not been fully examined, preliminary indications suggest that this may be the cheapest way of building large networks of the type to be described.

T. V. Stations

With proper siting of receiving antennas, broadcast television stations might be used to form additional high data rate links in emergencies.

Non-Synchronous Satellites

The problem of building a reliable network using non-synchronous satellites is somewhat similar to that of building a communications network with unreliable links. When a satellite is overhead, the link is operative. When a satellite is not overhead, the link is out of service. Thus, such links are highly compatible with the type of system to be described.

VARIABLE DATA RATE LINKS

In a conventional circuit switched system each of the tandem links require matched transmission bandwidths. But, in the previous paper,* it was seen that in order to make fullest use of a digital link the post-error-removal data rate would have to vary as it is a function of noise level. The problem then is to build a communication network made up of links of variable data rate to use the communication resource most efficiently.

VARIABLE DATA RATE USERS

Not only will the links of a digital data transmission operate at a variable data rate, so will the users. Many digital transmission applications are highly intermittent in nature, with each potential network user varying his demand from instant to instant. For example, if one transmitted one line of a 60 w.p.m. teletype message over a high-data "express route" operating at 1,500,000 bits per second, a 1/3 millisecond burst would be sent every 12 seconds. Where high data rate transmission links serve many subscribers on a time division basis, both the user and the network links will appear to be operating at a highly variable data rate.

---

*See footnote, p. 1.

COMMON USER

In communications, as in transportation, it is most economic for many users to share a common resource rather than each to build his own system--particularly when supplying intermittent or occasional service. This intermittency of service is highly characteristic of digital communication requirements. Therefore, we would like to consider the interconnection, one day, of many all digital links to provide a resource optimized for the handling of data for many potential intermittent users--a new common-user system.

Figure 9 demonstrates the basic notion. A wide mixture of different digital transmission links is combined to form a common resource divided among many potential users. But, each of these communications links could possibly have a different data rate. How can links of different data rates be interconnected?

USE OF STANDARD MESSAGE BLOCK

Present common carrier communications networks, used for digital transmission, use links and concepts originally designed for another purpose--voice. These systems are built around a frequency division multiplexing link-to-link interface standard. The standard between links is that of data rate. Time division multiplexing appears so natural to data transmission that we might wish to

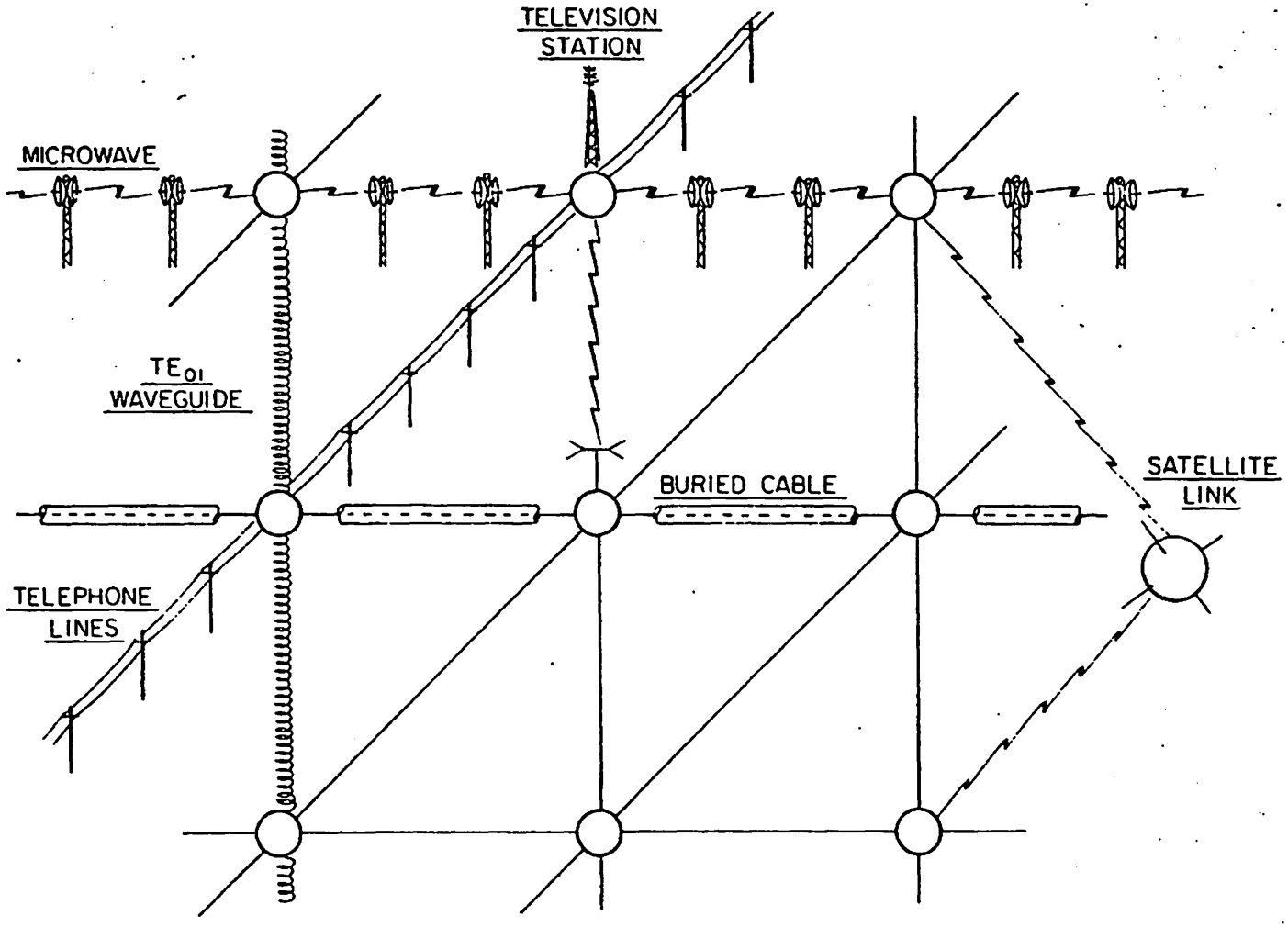


FIG. 9 – All Digital Network Composed of Mixture of Links

consider an alternative approach--a standardized message block as a network interface standard. While a standardized message block is common in many computer-communications applications, no serious attempt has ever been made to use it as a universal standard. A universally standardized message block would be composed of perhaps 1024 bits. Most of the message block would be reserved for whatever type data is to be transmitted, while the remainder would contain housekeeping information such as error detection and routing data, as in Fig. 10.

As we move to the future, there appears to be an increasing need for a standardized message block for our all-digital communications networks. As data rates increase, the velocity of propagation over long links becomes an increasingly important consideration.* We soon reach a point where more time is spent setting the switches in a conventional circuit switched system for short holding-time messages than is required for actual transmission of the data.

Most importantly, standardized data blocks permit many simultaneous users each with widely different bandwidth requirements to economically share a broadband network made up of varied data rate links.

---

*3000 miles at $\simeq$ 150,000 miles/sec. $\simeq$ 50 milliseconds transmission time, T.
1024-bit message at 1,500,000 bits/sec. $\simeq$ 2/3 millisecond message time, M.
$\therefore$ T>>M

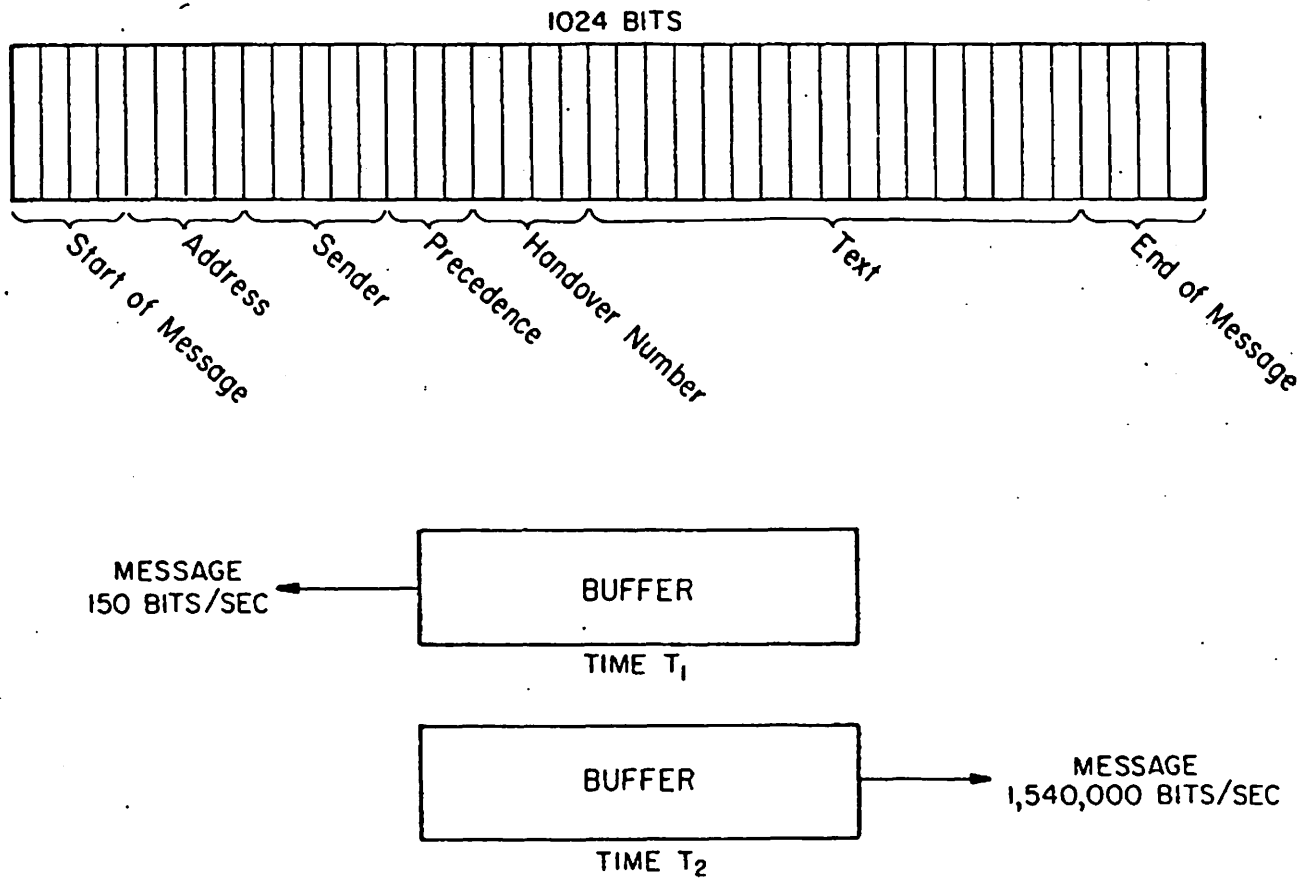


FIG. 10 — Message Block

The standardized message block simplifies construction of very high speed switches. Every user connected to the network can feed data at any rate up to a maximum value. The user's traffic is stored until a full data block is received by the first station. This block is rubber stamped with a heading and return address, plus additional housekeeping information. Then, it is transmitted into the network.

SWITCHING

In order to build a network with the survivability properties shown in Fig. 4, we must use a switching scheme able to find any possible path that might exist after heavy damage. The routing doctrine should find the shortest possible path and avoid self-oscillatory or "ring-around-the-rosey" switching.

We shall explore the possibilities of building a "real-time" data transmission system using store and forward techniques. The high data rates of the future carry us into a hybrid zone between store-and-forward and circuit switching. The system to be described is clearly store-and-forward if one examines the operations at each node singularly. But, the network user who has called up a "virtual connection" to an end station and has transmitted messages across the United States in a fraction of a second might also view the system as a black box providing

an apparent circuit connection across the U.S. There are two requirements that must be met to build such a quasi-real time system. First, the in-transit storage at each node should be minimized to prevent undesirable time delays. Secondly, the shortest instantaneously available path through the network should be found with the expectation that the status of the network will be rapidly changing. Microwave would be subject to fading interruptions and there would be rapid moment-to-moment variations in input loading. These problems place difficult requirements upon the switching. However, the development of digital computer technology has advanced so rapidly that it now appears possible to satisfy these requirements by a moderate amount of digital equipment. What is envisioned is a network of unmanned digital switches implementing a self-learning policy at each node so that overall traffic is effectively routed in a changing environment--without need for a central and possibly vulnerable control point. One particularly simple routing scheme examined is called the "hot-potato" heuristic routing doctrine and will be described in detail.

Torn-tape telegraph repeater stations and our mail system provide examples of conventional store-and-forward switching systems. In these systems, messages are relayed from station-to-station and stacked until the "best" outgoing link is free. The key feature of store-and-

forward transmission is that it allows a high line occupancy factor by storing so many messages at each node that there is a backlog of traffic awaiting transmission. But, the price for link efficiency is the price paid in storage capacity and time delay. However, it was found that most of the advantages of store-and-forward switching could be obtained with extremely little storage at the nodes.

Thus, in the system to be described, each node will attempt to get rid of its messages by choosing alternate routes if its preferred route is busy or destroyed. Each message is regarded as a "hot potato," and the nodes are not wearing gloves. Rather than hold the "hot potato," the node tosses the message to its neighbor, who will now try to get rid of the message.

THE POSTMAN

The switching process in any store-and-forward system is analogous to a postman sorting mail. A postman sits at each switching node. Messages arrive simultaneously from all links. The postman records bulletins describing the traffic loading status for each of the outgoing links. With proper status information, the postman is able to determine the best direction to send out any letters. So far, this mechanism is general and applicable to all store-and-forward communication systems.

HOT-POTATO HEURISTIC ROUTING DOCTRINE

To achieve real-time operation it is desirable to respond to change in network status as quickly as possible so we shall seek to derive the network status information directly into each message block.

Each standardized message block contains a "to" address, a "from" address, a handover number tag, and error detecting bits together with other housekeeping data. The message block is analogous to a letter. The "from" address is equivalent to the return address of the letter.

The handover number is a tag in each message block set to zero upon initial transmission of the message block into the network. Every time the message block is passed on, the handover number is incremented. The handover number tag on each message block indicates the length of time in the network or path length. This tag is somewhat analogous to the cancellation date of a conventional letter.

INDUCTIVE DETERMINATION OF BEST PATH

Assuming symmetrical bi-directional links, the postman can infer the "best" paths to transmit mail to any station merely by looking at the cancellation time or the equivalent handover number tag. If the postman sitting in the center of the United States received letters from San Francisco, he would find that letters from San Francisco arriving from channels to the west would come in with later cancellation dates than if such letters had

arrived in a roundabout manner from the east. Each letter carries an implicit indication of its length of transmission path. The astute postman can then deduce that the best channel to send a message to San Francisco is probably the link associated with the latest cancellation dates of messages from San Francisco. By observing the cancellation dates for all letters in transit, information is derived to route future traffic. The return address and cancellation date of recent letters is sufficient to determine the best direction to which to send subsequent letters.

THE HANDOVER NUMBER TABLE

While cancellation dates could conceivably be used on digital messages, it is more convenient to think in terms of a simpler digital analogy--a tag affixed to each message and incremented every time the message is relayed. Figure 11 shows the handover table located in the memory of a single node. A row is reserved for each major station of the network allowed to generate traffic. A column is assigned to each separate link connected to a node. As it was shown that redundancy levels on the order of four can create extremely "tough" networks and additional redundancy brought little, only about eight columns are really needed.

	LINK NUMBER							
	1	2	3	4	5	6	7	8
	HANDOVER NUMBER ENTRIES							
A	22	α	12	10	9	9	8	13
B	5	3	2	2	4	5	12	2
C	7	8	13	9	22	10	7	8
D	21	23	19	21	12	10	12	13
E	7	10	12	14	12	13	13	15
F	7	10	12	13	14	21		
G	6	4	10					
Z	15	20	7	3	10	8	5	10

BEST CHOICE				
1st	2nd	3rd	4th	5th
LINK NUMBER for DECISION CHOICE				
7	5	6	4	3
3	4	8	2	6
1	7	2	8	4
6	5	7	8	3
1	2	3	5	6
1	2	3	4	5
5	2	1	6	
4	7	3	6	

FIG. 11 — The Handover Number Table

PERFECT LEARNING

If the network used perfectly reliable, error free links, we might fill out our table in the following manner. Initially, set entries on the table to high values. Examine the handover number of each message arriving on each line for each station. If the observed handover number is less than the value already entered on the handover number table, change the value to that of the observed handover number. If the handover number of the message is greater than the value on the table, do nothing. After a short time this procedure will shake down the table to indicate the path length to each of the stations over each of the links connected to neighboring stations. This table can now be used to route new traffic. For example, if one wished to send traffic to station C, he would examine the entries for the row listed for station C based on traffic from C. Select the link corresponding to the column with the lowest handover number. This is the shortest path to C. If this preferred link is busy, do not wait, choose the next best link that is free.

DIGITAL SIMULATION OF PERFECT LEARNING

This basic routing procedure was tested by a Monte Carlo simulation of a 7x7 array of stations.* All tables were started completely blank to simulate a worst-case starting condition where no station knew the location of any other station. Within ½ second of simulated real world time, the network had learned the locations of all connected stations and was routing traffic in an efficient manner. The mean measured path length compared very favorably to the absolute shortest possible path length under various traffic loading conditions. Preliminary results indicate that network loadings on the order of 50 per cent of link capacity could be inserted without undue increase of path length. When local busy spots occur in the network, locally generated traffic is intermittently restrained from entering the busy points while the potential traffic jams clear. Thus, to the user, the network appears to be a variable data rate system. If the network is carrying light traffic, any new input line into the network would accept full traffic up to 1.5 million bits per second. But, if every station had heavy traffic and the network became heavily loaded, the total allowable input data rate from any single station in the network might

*Paul Baran and Sharla Boehm, Simulation of a Hot Potato Routing Doctrine (U), The RAND Corporation, RM-3103, (In preparation).

drop to perhaps 0.5 million bits per second. The absolute minimum guaranteed data capacity into the network from any station is a function of the location of the station in the network, redundancy level, and the mean path length of transmitted traffic in the network. The "choking" of input procedure has been simulated in the network and no signs of instability under overload noted. It was found that most of the advantage of store-and-forward transmission can be provided in a system having relatively little memory capacity. The network "guarantees" delivery of all traffic that it has accepted from a user.

FORGETTING AND IMPERFECT LEARNING

We have briefly considered network behavior when all links are working. But, we are also interested in determining network behavior with real world links--some destroyed, while others are being repaired. The network can be made rapidly responsive to the effects of destruction, repair, and transmission fades by a slight modification of the rules for computing the values on the handover number table. In the previous example, the lowest handover number ever encountered for a given origination, or "from" station, and over each link, was the value recorded in the handover number table. But, if some links had failed, our table would not have responded to the change. Thus, we must be more responsive to recent measurements

than old ones. This effect can be included in our calculation by the following policy. Take the most recently measured value of handover number; subtract the previous value found in the handover table; if the difference is positive, add a fractional part of this difference to the table value to form the updated table value. This procedure merely implements a "forgetting" procedure--placing more belief upon more recent measurements and less on old measurements. This device would, in the case of network damage, automatically modify the handover number table entry so as to exponentially and asymptotically approach the true shortest path value. If the difference between measured value minus the table value is negative, the new table value would change by only a fractional portion of the recently measured difference.

This implements a form of sceptical learning. Learning will take place even with occasional errors. Thus, by the simple device of using only two separate "learning constants," depending whether the measured value is greater or less than the table value, we can provide a mechanism that permits the network routing to be responsive to varying loads, breaks, and repairs. This learning and forgetting technique has been simulated for a few limited cases and was found to work well.

ADAPTATION TO ENVIRONMENT

This simple simultaneous learning and forgetting mechanism implemented independently at each node causes the entire network to suggest the appearance of an adaptative system responding to gross changes of environment in several respects, without human intervention. For example, consider self-adaptation to station location. A station, Able, normally transmitted from one location in the network, as shown in Fig. 12 (a). If Able moved to the location shown in Fig. 12 (b), all he need do to announce his new location is to transmit a few seconds of dummy traffic. The network will quickly relearn the new location and direct traffic toward Able at his new location. The links could also be cut and altered, yet the network would relearn. Each node sees its environment through myopic eyes by only having links and link status information to a few neighbors. There is no central control; only a simple local routing policy is performed at each node, yet the overall system adapts.

LOWEST COST PATH

We seek to provide the lowest cost path for data to be transmitted between users. When we consider complex networks, perhaps spanning continents, we encounter the problem of building networks with links of widely different data rates. How can paths be taken to encourage

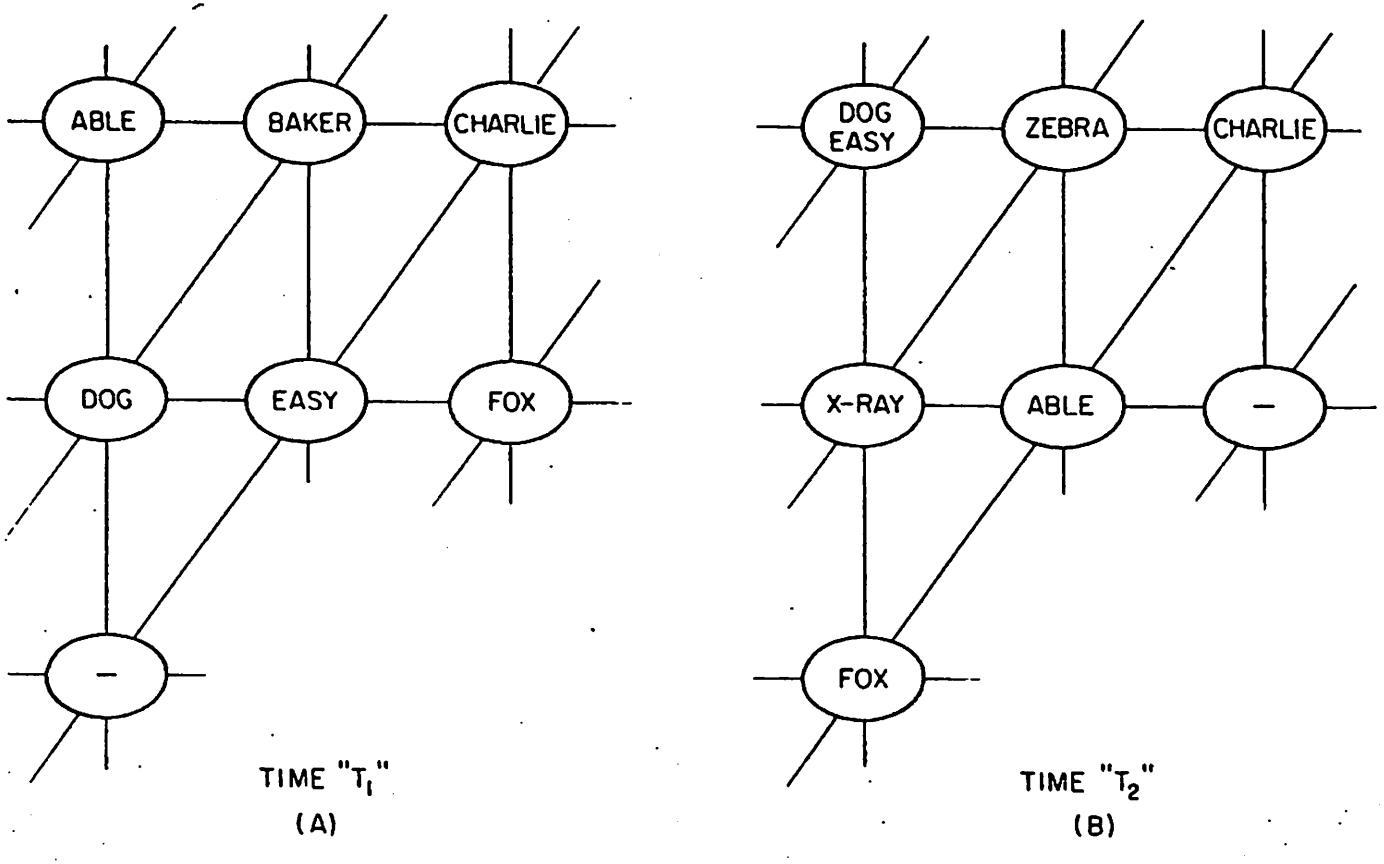


FIG. 12 – Adaptability to Change of User Location

most use of the least expensive links? The fundamentally simple adaptation technique can again be used. Instead of incrementing the handover by a fixed amount, each time a message is relayed, set the increment to correspond to link cost/bit of the transmission link. Thus, instead of the "instantaneously shortest non-busy path" criterion, the path taken will be that offering the cheapest transportation cost from user to user that is available. The technique can be further extended by placing priority and cost bounds in the message block itself, permitting certain users more of the communication resource during periods of heavy network use.

WHERE WE STAND TODAY

Although it is premature at this time to know all the problems involved in such a network and understand all costs, there are reasons to suspect that we may not wish to build future digital communication networks exactly the same way the nation has built its analog telephone plant.

There is an increasingly repeated statement made that one day we will require more capacity for data transmission than needed for voice. If this statement is correct, then it would appear prudent to broaden our planning consideration to include new concepts for future data network directions. Otherwise, we may stumble into being boxed in with the

uncomfortable restraints of communications links and switches originally designed for high quality analog transmission. New digital computer techniques using redundancy make cheap unreliable links potentially usable. Some sort of a switched network compatible with these links appears appropriate to meet this new upcoming demand for digital service.

Of course, we could use our existing circuit switching techniques. But, a system with greater capacity than the long lines of telephone plants might best be designed for such data transmission and survivability at the outset. Such a system should economically permit switching of very short blocks of data from a large number of users simultaneously with intermittent large volumes among a smaller set of points. Considering the size of the market there appears to be an incommensurately small amount of thinking about a national data plant designed primarily for data.

Is it time now to start thinking about a new and possibly non-existant public utility, a common user digital data communication plant designed specifically for the transmission of digital data among a large set of subscribers?

Is it time to consider the detailed format of a standard message block as a possible new data standard of the future?

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix H

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, Plaintiff, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	No. 1:15-cv-00662-TSE

OBJECTIONS AND RESPONSES BY DEFENDANTS NATIONAL SECURITY AGENCY AND ADM. MICHAEL S. ROGERS, DIRECTOR, TO PLAINTIFF'S FIRST AND SECOND SETS OF REQUESTS FOR ADMISSION

Pursuant to Rule 36 of the Federal Rules of Civil Procedure and District of Maryland Local Rule 104, Defendants National Security Agency ("NSA") and Adm. Michael S. Rogers, Director of the NSA, in his official capacity (together, the "NSA Defendants"), by their undersigned attorneys, object and respond as follows to Plaintiff Wikimedia Foundation's first and second sets of Requests for Admission, dated November 7 and 29, 2017, respectively.

GENERAL OBJECTIONS AND OBJECTIONS TO DEFINITIONS AND INSTRUCTIONS

1. The NSA Defendants object to Plaintiff's Requests for Admission to the extent, as set forth in response to specific requests below, that they are improper attempts to use requests for admission as discovery devices, specifically, as interrogatories.

2. The NSA Defendants object to Plaintiff's Requests for Admission to the extent, as set forth in response to specific requests below, that they seek information regarding the intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a).

3. The NSA Defendants object to Plaintiff's Requests for Admission to the extent, as set forth in response to specific requests below, they seek information that is irrelevant to jurisdictional issues, which are the only matters as to which the Court has authorized discovery in this case. *See* October 3, 2017, Order, ECF No. 117 at 1.

4. As set forth in response to specific requests below, the NSA Defendants object to the definition of the term "Circuit" as vague and ambiguous insofar as it is meant, by its reference to the use of that term in the Privacy and Civil Liberties Oversight Board's "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act" (the "PCLOB Section 702 Report") to assign the term "Circuit" a meaning other than its ordinary meaning in the telecommunications industry. The PCLOB is an independent agency within the Executive Branch, and the NSA Defendants do not have information regarding what, if anything, that entity intended by the term "Circuit" beyond the ordinary meaning of that term within the telecommunications industry as understood by the NSA Defendants.

5. As set forth in response to specific requests below, the NSA Defendants object to the definition of the term "Internet Transaction" as vague and ambiguous insofar as it is meant, by its reference to the use of that term in the PCLOB Section 702 Report, to assign the term "Internet Transaction" a meaning other than that understood by the NSA Defendants. The PCLOB is an independent agency within the Executive Branch, and the NSA Defendants do not have information regarding what, if anything, that entity intended by the term "Internet Transaction" beyond the meaning of that term as understood by the NSA Defendants.

6. As set forth in response to specific requests below, the NSA Defendants object to the definition of "Review" as compound, unduly burdensome and oppressive, and so vague and ambiguous as to render specific requests in which it is used incapable of reasoned response.

7. As set forth in response to specific requests below, the NSA Defendants object to the definition of "Interacted With" as compound, and, insofar as it incorporates the definition of "Review," also as unduly burdensome and oppressive, and so vague and ambiguous as to render specific requests in which it is used incapable of reasoned response.

8. As set forth in response to specific requests below, the NSA Defendants object to Plaintiff's Requests for Admission to the extent that they seek information that is protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

9. The following objections and responses are based upon information currently known to the NSA Defendants, and they reserve the right to supplement or amend their objections and responses should additional or different information become available.

10. Nothing contained in the following objections and responses shall be construed as a waiver of any applicable objection or privilege as to any request or as a waiver of any objection or privilege generally. Inadvertent disclosure or unauthorized disclosure of information subject to a claim of privilege shall not be deemed a waiver of such privilege.

OBJECTIONS AND RESPONSES TO FIRST SET OF REQUESTS FOR ADMISSION

REQUEST FOR ADMISSION NO. 1: Admit that there are between 45 and 55 international submarine cables that carry INTERNET COMMUNICATIONS directly into or directly out of the UNITED STATES.

OBJECTION: The NSA Defendants object to Request for Admission No. 1 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 1 as unduly burdensome and oppressive insofar as it requests that the NSA Defendants produce information regarding the telecommunications infrastructure that is equally available to the Plaintiff as it is to the NSA Defendants from public sources.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that it is difficult to determine the exact number of international submarine telecommunications cables that carry Internet communications directly into or out of the United States, because it is not publicly known whether particular cables carry Internet communications as opposed to telephonic or private-network communications. The Federal Communications Commission, which issues licenses to own and operate submarine cables and associated cable landing stations located in the United States, most recently reported that approximately 45 privately owned trans-ocean fiber optic cables (also referred to in the report as cable systems) landing in the United States or its territories were in service as of December 31, 2015. *See* Federal Communications Commission, International Bureau Report, 2015 U.S. International Circuit Capacity Data (August 2017), at 4 & Tables 4(A) & 4(B) at T-5 to T-8, available at https://apps.fcc.gov/edocs_public/attachmatch/DOC-346376A2.pdf. Telecommunications market research and consulting firm Telegeography publishes an online Submarine Cable Landing Directory, https://www.telegeography.com/telecom-resources/submarine-cable-landing-directory, which lists 45-50 privately owned international undersea cable systems landing in the United States or its territories, many of which, however, contain multiple cables or legs. Telegeography also publishes online a map purporting to depict the international submarine cables connecting the United States with other nations as of December 11, 2017, available at https://www.submarinecablemap.com.

The NSA Defendants respond further that, according to data available from Telegeography, international submarine cables typically contain 2-8 pairs of fiber-optic cables. Each fiber-optic pair is typically capable of carrying between approximately 15 and 120 individual communications circuits on different light wavelengths, depending on age and technology used. As a result, an individual submarine cable may carry between approximately

30 and 960 communications circuits. (Individual circuits may be subdivided further to create multiple "virtual circuits" through application of various technologies.) Each wavelength carried on a fiber-optic pair is typically capable of transporting between 10 and 100 gigabits of data per second (10-100 Gbps), meaning that a typical submarine cable can carry between approximately 300 and 96,000 Gbps of data.

REQUEST FOR ADMISSION NO. 2: Admit that the international submarine cables that carry INTERNET COMMUNICATIONS directly into or directly out of the UNITED STATES make landfall at approximately 40 to 45 different landing points within the UNITED STATES.

OBJECTION: The NSA Defendants object to Request for Admission No. 2 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 2 as unduly burdensome and oppressive insofar as it requests that NSA Defendants produce information regarding the telecommunications infrastructure that is equally available to the Plaintiff as it is to the NSA Defendants from public sources.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that, as noted in response to Request for Admission No. 1, above, it is not publicly known whether particular international submarine telecommunications cables carry Internet communications as opposed to telephonic or private-network communications, and it is therefore difficult as well to determine the exact number of points at which the cables carrying Internet communications make landfall within the United States. Telegeography's online Submarine Cable Landing Directory, https://www.telegeography.com/telecom-resources/submarine-cable-landing-directory, indicates that international undersea cable systems currently in service make landfall within the territory of the United States at approximately 75-80 locations.

REQUEST FOR ADMISSION NO. 3: Admit that the INTERNET BACKBONE includes international submarine cables that carry INTERNET COMMUNICATIONS into and out of the UNITED STATES.

OBJECTION: The NSA Defendants object to Request for Admission No. 3 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 3 as unduly burdensome and oppressive insofar as it requests that NSA Defendants produce information regarding the telecommunications infrastructure that is equally available to the Plaintiff as it is to the NSA Defendants from public sources.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that yes, the Internet backbone includes but is not limited to international submarine telecommunications cables that carry Internet communications.

REQUEST FOR ADMISSION NO. 4: Admit that the INTERNET BACKBONE includes high-capacity terrestrial cables that carry traffic within the UNITED STATES.

OBJECTION: The NSA Defendants object to Request for Admission No. 4 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 4 as unduly burdensome and oppressive insofar as it requests that NSA Defendants produce information regarding the telecommunications infrastructure that is equally available to the Plaintiff as it is to the NSA Defendants from public sources.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that yes, the Internet backbone includes but is not limited to high-capacity terrestrial telecommunications cables that carry Internet communications within the United States.

REQUEST FOR ADMISSION NO. 5: Admit that, in conducting Upstream surveillance, the NSA COPIES INTERNET COMMUNICATIONS that are in transit on the INTERNET BACKBONE, prior to RETAINING INTERNET COMMUNICATIONS that contain a SELECTOR.

OBJECTION: The NSA Defendants object to Request for Admission No. 5 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 5 on the grounds that it seeks information (which can be neither confirmed nor denied) regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

REQUEST FOR ADMISSION NO. 6: Admit that, in conducting Upstream surveillance, the NSA REVIEWS the contents of INTERNET COMMUNICATIONS that are in transit on the INTERNET BACKBONE, prior to RETAINING INTERNET COMMUNICATIONS that contain a SELECTOR.

OBJECTION: The NSA Defendants object to Request for Admission No. 6 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 6 on the grounds that it seeks information regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

The NSA Defendants also object to Request for Admission No. 6 insofar as the definition of "Reviews," by encompassing so many fundamentally different actions, renders this request compound, unduly burdensome and oppressive, vague and ambiguous, and incapable of reasoned response.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that in the course of the Upstream Internet collection process, certain

Internet transactions transiting the Internet backbone networks of certain electronic communication service providers are filtered for the purpose of excluding wholly domestic communications; are then screened to identify for acquisition those transactions that are to or from persons targeted in accordance with the current NSA targeting procedures; and must pass through both the filter and the screen before they can be ingested into Government databases.

REQUEST FOR ADMISSION NO. 7: Admit that, in conducting Upstream surveillance, the NSA COPIES INTERNET COMMUNICATIONS in BULK that are in transit on the INTERNET BACKBONE.

OBJECTION: The NSA Defendants object to Request for Admission No. 7 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 7 on the grounds that it seeks information (which can be neither confirmed nor denied) regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

REQUEST FOR ADMISSION NO. 8: Admit that, in conducting Upstream surveillance, the NSA REVIEWS the contents of INTERNET COMMUNICATIONS in BULK that are in transit on the INTERNET BACKBONE.

OBJECTION: The NSA Defendants object to Request for Admission No. 8 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 8 on the grounds that it seeks information regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

The NSA Defendants also object to Request for Admission No. 8 insofar as the definition of "Reviews," by encompassing so many fundamentally different actions, renders this request compound, unduly burdensome and oppressive, vague and ambiguous, and incapable of reasoned response.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that in the course of the Upstream Internet collection process, certain Internet transactions transiting the Internet backbone networks of certain electronic communication service providers are filtered for the purpose of excluding wholly domestic communications; are then screened to identify for acquisition those transactions that are to or from persons targeted in accordance with the current NSA targeting procedures; and must pass through both the filter and the screen before they can be ingested into Government databases.

REQUEST FOR ADMISSION NO. 9: Admit that, in conducting Upstream surveillance, the NSA COPIES INTERNET COMMUNICATIONS that are neither to nor from TARGETS, prior to RETAINING INTERNET COMMUNICATIONS that contain a SELECTOR.

OBJECTION: The NSA Defendants object to Request for Admission No. 9 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 9 on the grounds that it seeks information (which can be neither confirmed nor denied) regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. §3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

REQUEST FOR ADMISSION NO. 10: Admit that, in conducting Upstream surveillance, the NSA REVIEWS the contents of INTERNET COMMUNICATIONS that are neither to nor from TARGETS, prior to RETAINING INTERNET COMMUNICATIONS that contain a SELECTOR.

OBJECTION: The NSA Defendants object to Request for Admission No. 10 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 10 on the grounds that it seeks information regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

The NSA Defendants also object to Request for Admission No. 10 insofar as the definition of "Reviews," by encompassing so many fundamentally different actions, renders this request compound, unduly burdensome and oppressive, vague and ambiguous, and incapable of reasoned response.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that in the course of the Upstream Internet collection process, certain Internet transactions transiting the Internet backbone networks of certain electronic communication service providers are filtered for the purpose of excluding wholly domestic communications; are then screened to identify for acquisition those transactions that are to or from persons targeted in accordance with the current NSA targeting procedures; and must pass through both the filter and the screen before they can be ingested into Government databases.

REQUEST FOR ADMISSION NO. 11: Admit that the NSA does not consider an INTERNET COMMUNICATION "collected," within the meaning of the 2014 NSA Minimization Procedures, until after it has REVIEWED the contents of the communication and has selected it for RETENTION.

OBJECTION: The NSA Defendants object to Request for Admission No. 11 as an improper attempt to use a request for admission as a discovery device, specifically, as an

interrogatory. The NSA Defendants also object to Request for Admission No. 11 because what the NSA "consider[s]" the collection of an Internet communication to be, within the meaning of the 2014 NSA Section 702 Minimization Procedures or otherwise, is irrelevant to jurisdictional issues, which are the only matters as to which the Court has authorized discovery in this case. *See* October 3, 2017, Order, ECF No. 117 at 1.

The NSA Defendants also object to Request for Admission No. 11 to the extent that it seeks information regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1). Finally, the NSA Defendants object to Request for Admission No. 11 insofar as the definition of "Reviews," by encompassing so many fundamentally different actions, renders this request compound, unduly burdensome and oppressive, vague and ambiguous, and incapable of reasoned response.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that the NSA considers the term "collection" as it applies to the Upstream Internet collection process, whether in the 2014 NSA Section 702 Minimization Procedures or otherwise, to be the ingestion of Internet transactions into Government databases after they have been filtered for the purpose of excluding wholly domestic communications, and then screened to identify for acquisition those transactions that are to or from persons targeted in accordance with the current NSA targeting procedures.

REQUEST FOR ADMISSION NO. 12: Admit that, in the course of Upstream surveillance, the NSA RETAINS WHOLLY DOMESTIC COMMUNICATIONS.

OBJECTION: The NSA Defendants object to Request for Admission No. 12 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 12 because it

seeks information that is irrelevant to jurisdictional issues, which are the only matters as to which the Court has authorized discovery in this case. *See* October 3, 2017, Order, ECF No. 117 at 1.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants admit that, as found by the Privacy and Civil Liberties Oversight Board, technical measures taken to prevent acquisition of wholly domestic communications in the Upstream Internet collection process do not operate perfectly. However, the current NSA Section 702 Minimization Procedures require that wholly domestic communications "be promptly destroyed upon recognition," subject to limited exceptions described in Section 5 therein.

REQUEST FOR ADMISSION NO. 13: Admit that the NSA conducts Upstream surveillance on multiple INTERNET BACKBONE CIRCUITS.

OBJECTION: The NSA Defendants object to Request for Admission No. 13 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 13 on the grounds that it seeks information (which can be neither confirmed nor denied) regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

REQUEST FOR ADMISSION NO. 14: Admit that the NSA conducts Upstream surveillance on multiple "international Internet link[s]," as that term is used by the government in its submission to the Foreign Intelligence Surveillance Court, titled "Government's Response to the Court's Briefing Order of May 9, 2011," and filed on June 1, 2011, *see* [*Redacted*], 2011 WL 10945618, at *15 (FISC Oct. 3, 2011).

OBJECTION: The NSA Defendants object to Request for Admission No. 14 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants also object to Request for Admission No. 14 on the ground

that it attributes the phrase "international Internet link" to a Government document when in fact the phrase is taken from an opinion of the Foreign Intelligence Surveillance Court that does not purport to quote directly from the referenced Government document. *See* [*Redacted*], 2011 WL 10945618, at *15 (FISC Oct. 3, 2011). Whether the phrase "international Internet link" is contained within the referenced Government document is information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. §3605(a).

The NSA Defendants further object to Request for Admission No. 14 on the grounds that it seeks information (which can be neither confirmed nor denied) regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

REQUEST FOR ADMISSION NO. 15: Admit that the NSA conducts Upstream surveillance at multiple INTERNET BACKBONE "chokepoints" or "choke points" (as that term is used by YOU).

OBJECTION: The NSA Defendants object to Request for Admission No. 15 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants also object to Request for Admission No. 15 as vague and ambiguous insofar as it does not specify where or in what context the NSA Defendants allegedly use the term "chokepoints" or "choke points." To the extent that Plaintiff's reference to that term alludes to what is described in the Amended Complaint as an "NSA slide," *see* Am. Compl. ¶ 68, the NSA Defendants object to this request as implicitly seeking information (which can be neither confirmed nor denied) regarding the authenticity of the purported slide, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

The NSA Defendants further object to Request for Admission No. 15 on the grounds that it seeks information (which can be neither confirmed nor denied) regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

REQUEST FOR ADMISSION NO. 16: Admit that the document attached hereto as Exhibit A, titled "Why are we interested in HTTP?," is a true and correct excerpted copy of a genuine document.

OBJECTION: The NSA Defendants object to Request for Admission No. 16 as irrelevant, and as vague and ambiguous insofar as it does not specify what kind of document Plaintiff claims Exhibit A "genuine[ly]" to be. To the extent that Plaintiff seeks to establish the authenticity of Exhibit A as evidence of intelligence activities allegedly conducted by the NSA, Defendants also object to Request for Admission No. 16 on the grounds that it seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

REQUEST FOR ADMISSION NO. 17: Admit that the statements within the document attached hereto as Exhibit A were made by YOUR employees on matters within the scope of their employment during the course of their employment.

OBJECTION: The NSA Defendants object to Request for Admission No. 17 as irrelevant, and, to the extent Plaintiff seeks to establish the admissibility of statements made in Exhibit A as evidence of intelligence activities allegedly conducted by the NSA, on the grounds that this request seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

REQUEST FOR ADMISSION NO. 18: Admit that statements within the document attached hereto as Exhibit A were made by persons YOU authorized to make statements on the subjects of the statements within the document.

OBJECTION: The NSA Defendants object to Request for Admission No. 18 as irrelevant, and, to the extent Plaintiff seeks to establish the admissibility of statements made in Exhibit A as evidence of intelligence activities allegedly conducted by the NSA, on the ground that this request seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

REQUEST FOR ADMISSION NO. 19: Admit that the document attached hereto as Exhibit B, titled "Fingerprints and Appids," and "Fingerprints and Appids (more)," is a true and correct excerpted copy of a genuine document.

OBJECTION: The NSA Defendants object to Request for Admission No. 19 as irrelevant, and as vague and ambiguous insofar as it does not specify what kind of document Plaintiff claims Exhibit B "genuine[ly]" to be. To the extent that Plaintiff seeks to establish the authenticity of Exhibit B as evidence of intelligence activities allegedly conducted by the NSA, Defendants also object to Request for Admission No. 19 on the grounds that it seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

REQUEST FOR ADMISSION NO. 20: Admit that the statements within the document attached hereto as Exhibit B were made by YOUR employees on matters within the scope of their employment during the course of their employment.

OBJECTION: The NSA Defendants object to Request for Admission No. 20 as irrelevant, and, to the extent Plaintiff seeks to establish the admissibility of statements made in Exhibit B as evidence of intelligence activities allegedly conducted by the NSA, on the ground that this request seeks information (which can be neither confirmed nor denied) that is protected

from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

REQUEST FOR ADMISSION NO. 21: Admit that statements within the document attached hereto as Exhibit B were made by persons YOU authorized to make statements on the subjects of the statements within the document.

OBJECTION: The NSA Defendants object to Request for Admission No. 21 as irrelevant, and, to the extent Plaintiff seeks to establish the admissibility of statements made in Exhibit B as evidence of intelligence activities allegedly conducted by the NSA, on the ground that this request seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

REQUEST FOR ADMISSION NO. 22: Admit that the document attached hereto as Exhibit C, "Seven Access Sites—International 'Choke Points'," is a true and correct excerpted copy of a genuine document.

OBJECTION: The NSA Defendants object to Request for Admission No. 22 as irrelevant, and as vague and ambiguous insofar as it does not specify what kind of document Plaintiff claims Exhibit C "genuine[ly]" to be. To the extent that Plaintiff seeks to establish the authenticity of Exhibit C as evidence of intelligence activities allegedly conducted by the NSA, Defendants also object to Request for Admission No. 22 on the grounds that it seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

REQUEST FOR ADMISSION NO. 23: Admit that the statements within the document attached hereto as Exhibit C were made by YOUR employees on matters within the scope of their employment during the course of their employment.

OBJECTION: The NSA Defendants object to Request for Admission No. 23 as irrelevant, and, to the extent Plaintiff seeks to establish the admissibility of statements made in

Exhibit C as evidence of intelligence activities allegedly conducted by the NSA, on the ground that this request seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

REQUEST FOR ADMISSION NO. 24: Admit that statements within the document attached hereto as Exhibit C were made by persons YOU authorized to make statements on the subjects of the statements within the document.

OBJECTION: The NSA Defendants object to Request for Admission No. 24 as irrelevant, and, to the extent Plaintiff seeks to establish the admissibility of statements made in Exhibit C as evidence of intelligence activities allegedly conducted by the NSA, on the ground that this request seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

REQUEST FOR ADMISSION NO. 25: Admit that the document attached hereto as Exhibit D, titled "SSO's Support to the FBI for Implementation of their Cyber FISA Orders," is a true and correct copy of a genuine document.

OBJECTION: The NSA Defendants object to Request for Admission No. 25 as irrelevant, and as vague and ambiguous insofar as it does not specify what kind of document Plaintiff claims Exhibit D "genuine[ly]" to be. To the extent that Plaintiff seeks to establish the authenticity of Exhibit D as evidence of intelligence activities allegedly conducted by the NSA, Defendants also object to Request for Admission No. 25 on the grounds that it seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

REQUEST FOR ADMISSION NO. 26: Admit that the statements within the document attached hereto as Exhibit D were made by YOUR employees on matters within the scope of their employment during the course of their employment.

OBJECTION: The NSA Defendants object to Request for Admission No. 26 as irrelevant, and, to the extent Plaintiff seeks to establish the admissibility of statements made in Exhibit D as evidence of intelligence activities allegedly conducted by the NSA, on the ground that this request seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

REQUEST FOR ADMISSION NO. 27: Admit that statements within the document attached hereto as Exhibit D were made by persons YOU authorized to make statements on the subjects of the statements within the document.

OBJECTION: The NSA Defendants object to Request for Admission No. 27 as irrelevant, and, to the extent Plaintiff seeks to establish the admissibility of statements made in Exhibit D as evidence of intelligence activities allegedly conducted by the NSA, on the ground that this request seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

REQUEST FOR ADMISSION NO. 28: Admit that the document attached hereto as Exhibit E, titled "Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended" and dated July 28, 2009 (the "NSA Targeting Procedures") is a true and correct copy of a genuine document.

OBJECTION: To the extent that Plaintiff seeks to establish the authenticity of Exhibit E as evidence of targeting procedures allegedly used by the NSA in 2009, the NSA Defendants object to Request for Admission No. 28 (i) as irrelevant to jurisdictional issues, which are the only matters as to which the Court has authorized discovery in this case, *see*

October 3, 2017, Order, ECF No. 117 at 1, (ii) as irrelevant, in particular, to Plaintiff's standing to seek prospective relief, and (iii) on the ground that it seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

REQUEST FOR ADMISSION NO. 29: Admit that the statements within the document attached hereto as Exhibit E were made by YOUR employees on matters within the scope of their employment during the course of their employment.

OBJECTION: To the extent Plaintiff seeks to establish the admissibility of statements made in Exhibit E as evidence of intelligence activities allegedly conducted by the NSA in 2009, the NSA Defendants object to Request for Admission No. 29 as irrelevant and on the grounds that it seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

REQUEST FOR ADMISSION NO. 30: Admit that statements within the document attached hereto as Exhibit E were made by persons YOU authorized to make statements on the subjects of the statements within the document.

OBJECTION: To the extent Plaintiff seeks to establish the admissibility of statements made in Exhibit E as evidence of intelligence activities allegedly conducted by the NSA in 2009, the NSA Defendants object to Request for Admission No. 30 as irrelevant and on the grounds that it seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

REQUEST FOR ADMISSION NO. 31: Admit that the document attached hereto as Exhibit F, titled "Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended," dated July 2014, and available at https://www.dni.gov/files/documents/0928/2014%20NSA%20702%20Minimization%20Procedures.pdf, is a true and correct copy of a genuine document.

OBJECTION: The NSA Defendants object to Request for Admission No. 31 as irrelevant to jurisdictional issues, which are the only matters as to which the Court has authorized discovery in this case. *See* October 3, 2017, Order, ECF No. 117 at 1.

RESPONSE: Subject to the objection stated above, and without waiving it, the NSA Defendants admit that Exhibit 1 hereto is a true and correct (public) copy of the "Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended," dated July 2014, and available at https://www.dni.gov/files/documents/0928/2014%20NSA%20702%20Minimization%20Procedures.pdf.

REQUEST FOR ADMISSION NO. 32: Admit that the statements within the document attached hereto as Exhibit F were made by YOUR employees on matters within the scope of their employment during the course of their employment.

OBJECTION: The NSA Defendants object to Request for Admission No. 32 as irrelevant to jurisdictional issues, which are the only matters as to which the Court has authorized discovery in this case. *See* October 3, 2017, Order, ECF No. 117 at 1.

RESPONSE: Denied. The 2014 NSA Section 702 Minimization Procedures, Exhibit 1 hereto, were adopted by the Attorney General of the United States, in consultation with the Director of National Intelligence, as attested by the Attorney General's signature thereto.

REQUEST FOR ADMISSION NO. 33: Admit that statements within the document attached hereto as Exhibit F were made by persons YOU authorized to make statements on the subjects of the statements within the document.

OBJECTION: The NSA Defendants object to Request for Admission No. 33 as irrelevant to jurisdictional issues, which are the only matters as to which the Court has authorized discovery in this case. *See* October 3, 2017, Order, ECF No. 117 at 1.

RESPONSE: Denied. The 2014 NSA Section 702 Minimization Procedures, Exhibit 1 hereto, were adopted by the Attorney General of the United States, in consultation with the Director of National Intelligence, as attested by the Attorney General's signature thereto.

OBJECTIONS AND RESPONSES TO SECOND SET OF REQUESTS FOR ADMISSION

REQUEST FOR ADMISSION NO. 34: Admit that, in conducting Upstream surveillance, the NSA has COPIED at least one WIKIMEDIA INTERNET COMMUNICATION.

OBJECTION: The NSA Defendants object to Request for Admission No. 34 on the grounds that it seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privilege under 50 U.S.C. § 3024(i)(1). The NSA Defendants further object to Request for Admission No. 34 on the grounds that it seeks information regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a).

REQUEST FOR ADMISSION NO. 35: Admit that, in conducting Upstream surveillance, the NSA has REVIEWED the content of at least one WIKIMEDIA INTERNET COMMUNICATION.

OBJECTION: The NSA Defendants object to Request for Admission No. 35 on the grounds that it seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privilege under 50 U.S.C. § 3024(i)(1). The NSA Defendants further object to Request for Admission No. 35 on the

grounds that it seeks information regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a).

The NSA Defendants also object to Request for Admission No. 35 insofar as the definition of "Review[ed]," by encompassing so many fundamentally different actions, renders this request compound, unduly burdensome and oppressive, vague and ambiguous, and incapable of reasoned response.

REQUEST FOR ADMISSION NO. 36: Admit that, in conducting Upstream surveillance, the NSA has RETAINED at least one WIKIMEDIA INTERNET COMMUNICATION.

OBJECTION: The NSA Defendants object to Request for Admission No. 36 on the grounds that it seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privilege under 50 U.S.C. § 3024(i)(1). The NSA Defendants further object to Request for Admission No. 36 on the grounds that it seeks information regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a).

Dated: January 8, 2018

CHAD A. READLER
Acting Assistant Attorney General

ANTHONY J. COPPOLINO
Deputy Branch Director

/s/ James J. Gilligan
JAMES J. GILLIGAN
Special Litigation Counsel

RODNEY PATTON
Senior Trial Counsel

JULIA A. BERMAN
TIMOTHY A. JOHNSON
Trial Attorneys

U.S Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave., N.W., Room 6102
Washington, D.C. 20001
Phone: (202) 514-3358
Fax: (202) 616-8470
Email: james.gilligan@usdoj.gov

Counsel for the NSA Defendants

EXHIBIT 1

EXHIBIT B

MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED

(U) Section 1 - Applicability and Scope

(U) These National Security Agency (NSA) minimization procedures apply to the acquisition, retention, use, and dissemination of information, including non-publicly available information concerning unconsenting United States persons, that is acquired by targeting non-United States persons reasonably believed to be located outside the United States in accordance with section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended (FISA or "the Act").

(U) If NSA determines that it must take action in apparent departure from these minimization procedures to protect against an immediate threat to human life (e.g., force protection or hostage situations) and that it is not feasible to obtain a timely modification of these procedures, NSA may take such action immediately. NSA will report the action taken to the Office of the Director of National Intelligence and to the National Security Division of the Department of Justice, which will promptly notify the Foreign Intelligence Surveillance Court of such activity.

~~(S//NF)~~ Nothing in these procedures shall restrict NSA's performance of lawful oversight functions of its personnel or systems, or lawful oversight functions of the Department of Justice's National Security Division, Office of the Director of National Intelligence, or the applicable Offices of the Inspectors General. Additionally, nothing in these procedures shall restrict NSA's ability to conduct vulnerability or network assessments using information acquired pursuant to section 702 of the Act in order to ensure that NSA systems are not or have not been compromised. Notwithstanding any other section in these procedures, information used by NSA to conduct vulnerability or network assessments may be retained for one year solely for that limited purpose. Any information retained for this purpose may be disseminated only in accordance with the applicable provisions of these procedures.

(U) For the purposes of these procedures, the terms "National Security Agency" and "NSA personnel" refer to any employees of the National Security Agency/Central Security Service ("NSA/CSS" or "NSA") and any other personnel engaged in Signals Intelligence (SIGINT) operations authorized pursuant to section 702 of the Act if such operations are executed under the direction, authority, or control of the Director, NSA/Chief, CSS (DIRNSA).

(U) Section 2 - Definitions

(U) In addition to the definitions in sections 101 and 701 of the Act, the following definitions will apply to these procedures:

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: ~~20320108~~

(a) (U) Acquisition means the collection by NSA or the Federal Bureau of Investigation (FBI) through electronic means of a non-public communication to which it is not an intended party.

(b) (U) Communications concerning a United States person include all communications in which a United States person is discussed or mentioned, except where such communications reveal only publicly available information about the person.

(c) (U) Communications of a United States person include all communications to which a United States person is a party.

(d) (U) Consent is the agreement by a person or organization to permit the NSA to take particular actions that affect the person or organization. To be effective, consent must be given by the affected person or organization with sufficient knowledge to understand the action that may be taken and the possible consequences of that action. Consent by an organization will be deemed valid if given on behalf of the organization by an official or governing body determined by the General Counsel, NSA, to have actual or apparent authority to make such an agreement.

(e) (U) Foreign communication means a communication that has at least one communicant outside of the United States. All other communications, including communications in which the sender and all intended recipients are reasonably believed to be located in the United States at the time of acquisition, are domestic communications.

(f) (U) Identification of a United States person means (1) the name, unique title, or address of a United States person; or (2) other personal identifiers of a United States person when appearing in the context of activities conducted by that person or activities conducted by others that are related to that person. A reference to a product by brand name, or manufacturer's name or the use of a name in a descriptive sense, e.g., "Monroe Doctrine," is not an identification of a United States person.

(g) ~~(TS//SI//NF)~~ Internet transaction, for purposes of these procedures, means an Internet communication that is acquired through NSA's upstream collection techniques. An Internet transaction may contain information or data representing either a discrete communication [redacted] or multiple discrete communications [redacted]

(h) (U) Processed or processing means any step necessary to convert a communication into an intelligible form intended for human inspection.

(i) (U) Publicly available information means information that a member of the public could obtain on request, by research in public sources, or by casual observation.

(j) (U) Technical data base means information retained for cryptanalytic, traffic analytic, or signal exploitation purposes.

(k) (U) United States person means a United States person as defined in the Act. The following guidelines apply in determining whether a person whose status is unknown is a United States person:

(1) (U) A person known to be currently in the United States will be treated as a United States person unless positively identified as an alien who has not been admitted for permanent residence, or unless the nature or circumstances of the person's communications give rise to a reasonable belief that such person is not a United States person.

(2) (U) A person known to be currently outside the United States, or whose location is unknown, will not be treated as a United States person unless such person can be positively identified as such, or the nature or circumstances of the person's communications give rise to a reasonable belief that such person is a United States person.

(3) (U) A person who at any time has been known to have been an alien admitted for lawful permanent residence is treated as a United States person. Any determination that a person who at one time was a United States person (including an alien admitted for lawful permanent residence) is no longer a United States person must be made in consultation with the NSA Office of General Counsel.

(4) (U) An unincorporated association whose headquarters or primary office is located outside the United States is presumed not to be a United States person unless there is information indicating that a substantial number of its members are citizens of the United States or aliens lawfully admitted for permanent residence.

(U) Section 3 - Acquisition and Handling - General

(a) (U) Acquisition

(U) The acquisition of information by targeting non-United States persons reasonably believed to be located outside the United States pursuant to section 702 of the Act will be effected in accordance with an authorization made by the Attorney General and Director of National Intelligence pursuant to subsection 702(a) of the Act and will be conducted in a manner designed, to the greatest extent reasonably feasible, to minimize the acquisition of information not relevant to the authorized purpose of the acquisition.

(b) (U) Monitoring, Recording, and Handling

(1) (U) Personnel will exercise reasonable judgment in determining whether information acquired must be minimized and will destroy inadvertently acquired communications of or concerning a United States person at the earliest practicable point at which such communication can be identified either: as clearly not relevant to the authorized purpose of the acquisition (e.g., the communication does not contain foreign intelligence information); or, as not containing evidence of a crime which may be

disseminated under these procedures. Except as provided for in subsection 3(c) below, such inadvertently acquired communications of or concerning a United States person may be retained no longer than five years from the expiration date of the certification authorizing the collection in any event.

(2) (U) Communications of or concerning United States persons that may be related to the authorized purpose of the acquisition may be forwarded to analytic personnel responsible for producing intelligence information from the collected data. Such communications or information may be retained and disseminated only in accordance with Sections 3, 4, 5, 6, and 8 of these procedures.

(3) (U//~~FOUO~~) As a communication is reviewed, NSA analyst(s) will determine whether it is a domestic or foreign communication to, from, or about a target and is reasonably believed to contain foreign intelligence information or evidence of a crime for purposes of assessing how the communication should be handled in accordance with these procedures.

(4) (U) Handling of Internet Transactions Acquired Through NSA Upstream Collection Techniques

a. (~~TS//SI//NF~~) NSA will take reasonable steps post-acquisition to identify and segregate through technical means Internet transactions that cannot be reasonably identified as containing single, discrete communications where: the active user of the transaction (i.e., the electronic communications account/address/identifier used to send or receive the Internet transaction to or from a service provider) is reasonably believed to be located in the United States; or the location of the active user is unknown.

1. (~~TS//SI//NF~~) Notwithstanding subsection 3(b)(4)a. above, NSA may process Internet transactions acquired through NSA upstream collection techniques in order to render such transactions intelligible to analysts.

2. (~~TS//SI//NF~~) Internet transactions that are identified and segregated pursuant to subsection 3(b)(4)a. will be retained in an access-controlled repository that is accessible only to NSA analysts who have been trained to review such transactions for the purpose of identifying those that contain discrete communications as to which the sender and all intended recipients are reasonably believed to be located in the United States.

(a) (~~TS//SI//NF~~) Any information contained in a segregated Internet transaction (including metadata) may not be moved or copied from the segregated repository or otherwise used for foreign intelligence purposes unless it has been determined that the transaction does not contain any discrete communication as to which the sender and all intended recipients are reasonably believed to be located in the United States. Any Internet transaction that is identified and segregated pursuant to subsection

3(b)(4)a. and is subsequently determined to contain a discrete communication as to which the sender and all intended recipients are reasonably believed to be located in the United States will be handled in accordance with Section 5 below.

(b) (U//~~FOUO~~) Any information moved or copied from the segregated repository into repositories more generally accessible to NSA analysts will be handled in accordance with subsection 3(b)(4)b. below and the other applicable provisions of these procedures.

(c) (U//~~FOUO~~) Any information moved or copied from the segregated repository into repositories more generally accessible to NSA analysts will be marked, tagged, or otherwise identified as having been previously segregated pursuant to subsection 3(b)(4)a.

3. ~~(TS//SI//NF)~~ Internet transactions that are not identified and segregated pursuant to subsection 3(b)(4)a. will be handled in accordance with subsection 3(b)(4)b. below and the other applicable provisions of these procedures.

b. (U) NSA analysts seeking to use (for example, in a FISA application, intelligence report, or section 702 targeting) a discrete communication within an Internet transaction that contains multiple discrete communications will assess whether the discrete communication: 1) is a communication as to which the sender and all intended recipients are located in the United States; and 2) is to, from, or about a tasked selector, or otherwise contains foreign intelligence information.

1. ~~(TS//SI//NF)~~ If an NSA analyst seeks to use a discrete communication within an Internet transaction that contains multiple discrete communications, the analyst will first perform checks to determine the locations of the sender and intended recipients of that discrete communication to the extent reasonably necessary to determine whether the sender and all intended recipients of that communication are located in the United States. If an analyst determines that the sender and all intended recipients of a discrete communication within an Internet transaction are located in the United States, the Internet transaction will be handled in accordance with Section 5 below.

2. (U) If an NSA analyst seeks to use a discrete communication within an Internet transaction that contains multiple discrete communications, the analyst will assess whether the discrete communication is to, from, or about a tasked selector, or otherwise contains foreign intelligence information.

(a) (U) If the discrete communication is to, from, or about a tasked selector, any U.S. person information in that communication will be handled in accordance with the applicable provisions of these procedures.

(b) (U) If the discrete communication is not to, from, or about a tasked selector but otherwise contains foreign intelligence information, and the discrete communication is not to or from an identifiable U.S. person or a person reasonably believed to be located in the United States, that communication (including any U.S. person information therein) will be handled in accordance with the applicable provisions of these procedures.

(c) (U) If the discrete communication is not to, from, or about a tasked selector but is to or from an identifiable U.S. person, or a person reasonably believed to be located in the United States, the NSA analyst will document that determination in the relevant analytic repository or tool if technically possible or reasonably feasible. Such discrete communication cannot be used for any purpose other than to protect against an immediate threat to human life (e.g., force protection or hostage situations). NSA will report any such use to the Office of the Director of National Intelligence and to the National Security Division of the Department of Justice, which will promptly notify the Foreign Intelligence Surveillance Court of such use.

3. ~~(TS//SI//NF)~~ An NSA analyst seeking to use a discrete communication within an Internet transaction that contains multiple discrete communications in a FISA application, intelligence report, or section 702 targeting must appropriately document the verifications required by subsections 3(b)(4)b.1. and 2. above.

4. ~~(TS//SI//NF)~~ Notwithstanding subsection 3(b)(4)b. above, NSA may use metadata extracted from Internet transactions acquired on or after October 31, 2011, that are not identified and segregated pursuant to subsection 3(b)(4)a. without first assessing whether the metadata was extracted from: a) a discrete communication as to which the sender and all intended recipients are located in the United States; or b) a discrete communication to, from, or about a tasked selector. Any metadata extracted from Internet transactions that are not identified and segregated pursuant to subsection 3(b)(4)a. above will be handled in accordance with the applicable provisions of these procedures. Any metadata extracted from an Internet transaction subsequently determined to contain a discrete communication as to which the sender and all intended recipients are reasonably believed to be located inside the United States shall be destroyed upon recognition.

(5) (U) Magnetic tapes or other storage media containing communications acquired pursuant to section 702 may be scanned by computer to identify and select communications for analysis. Computer selection terms used for scanning, such as telephone numbers, key words or phrases, or other discriminators, will be limited to those selection terms reasonably likely to return foreign intelligence information. Identifiers of an identifiable U.S. person may not be used as terms to identify and select for analysis any Internet communication acquired through NSA's upstream

collection techniques. Any use of United States person identifiers as terms to identify and select communications must first be approved in accordance with NSA procedures. NSA will maintain records of all United States person identifiers approved for use as selection terms. The Department of Justice's National Security Division and the Office of the Director of National Intelligence will conduct oversight of NSA's activities with respect to United States persons that are conducted pursuant to this paragraph.

(6) (U) Further handling, retention, and dissemination of foreign communications will be made in accordance with Sections 4, 6, 7, and 8 as applicable, below. Further handling, storage, and dissemination of inadvertently acquired domestic communications will be made in accordance with Sections 4, 5, and 8 below.

(c) (U) Destruction of Raw Data

(1) ~~(S//SI~~ [redacted] Telephony communications and Internet communications acquired by or with the assistance of the FBI from Internet Service Providers that do not meet the retention standards set forth in these procedures and that are known to contain communications of or concerning United States persons will be destroyed upon recognition. Telephony communications and Internet communications acquired by or with the assistance of the FBI from Internet Service Providers may not be retained longer than five years from the expiration date of the certification authorizing the collection unless NSA specifically determines that each such communication meets the retention standards in these procedures.

(2) ~~(TS//SI//NF)~~ Internet transactions acquired through NSA's upstream collection techniques that do not contain any information that meets the retention standards set forth in these procedures and that are known to contain communications of or concerning United States persons will be destroyed upon recognition. An Internet transaction may not be retained longer than two years from the expiration date of the certification authorizing the collection unless NSA specifically determines that at least one discrete communication within the Internet transaction meets the retention standards in these procedures and that each discrete communication within the transaction either: (a) is to, from, or about a tasked selector; or (b) is not to, from, or about a tasked selector and is also not to or from an identifiable United States person or person reasonably believed to be in the United States. The Internet transactions that may be retained include those that were acquired because of limitations on NSA's ability to filter communications. Any Internet communications acquired through NSA's upstream collection techniques that are retained in accordance with this subsection may be reviewed and handled only in accordance with the standards set forth above in subsection 3(b)(4) of these procedures.

(3) ~~(TS//SI//NF)~~ Any Internet transactions acquired through NSA's upstream collection techniques prior to October 31, 2011, will be destroyed upon recognition.

(4) ~~(S//NF)~~ NSA may temporarily retain specific section 702-acquired information that would otherwise have to be destroyed, pursuant to section 3(a)-(c) above, if the Department of Justice advises NSA in writing that such information is subject to a preservation obligation in pending or anticipated administrative, civil, or criminal litigation. The specific information to be retained (including, but not limited to, the target(s) or selector(s) whose unminimized information must be preserved and the relevant time period at issue in the litigation), and the particular litigation for which the information will be retained, shall be identified in writing by the Department of Justice. Personnel not working on the particular litigation matter shall not access the unminimized section 702-acquired information preserved pursuant to a written preservation notice from the Department of Justice that would otherwise have been destroyed pursuant to these procedures. Other personnel shall only access the information being retained for litigation-related reasons on a case-by-case basis after consultation with the Department of Justice. The Department of Justice shall notify NSA in writing once the section 702-acquired information is no longer required to be preserved for such litigation matters, and then NSA shall promptly destroy the section 702-acquired information as otherwise required by these procedures. Circumstances could arise requiring that section 702-acquired information subject to other destruction/age off requirements in these procedures (e.g., Section 5) be retained because it is subject to a preservation requirement. In such cases the Government will notify the Foreign Intelligence Surveillance Court and seek permission to retain the material as appropriate consistent with law. Depending on the nature, scope and complexity of a particular preservation obligation, in certain circumstances it may be technically infeasible to retain certain section 702-acquired information. Should such circumstances arise, they will be brought to the attention of the court with jurisdiction over the underlying litigation matter for resolution.

(d) (U) Change in Target's Location or Status

(1) (U//~~FOUO~~) In the event that NSA reasonably believes that a target is located outside the United States and subsequently learns that the person is inside the United States, or if NSA concludes that a target who at the time of targeting was believed to be a non-United States person is in fact a United States person at the time of acquisition, the acquisition from that person will be terminated without delay.

(2) (U) Any communications acquired through the targeting of a person who at the time of targeting was reasonably believed to be located outside the United States but is in fact located inside the United States at the time such communications were acquired, and any communications acquired by targeting a person who at the time of targeting was believed to be a non-United States person but was in fact a United States person at the time such communications were acquired, will be treated as domestic communications under these procedures.

(e) ~~(S//NF)~~ In the event that NSA seeks to use any information acquired pursuant to section 702 during a time period when there is uncertainty about the location of the target of the acquisition because the [redacted] post-tasking checks described in NSA's section 702

targeting procedures were not functioning properly, NSA will follow its internal procedures for determining whether such information may be used (including, but not limited to, in FISA applications, section 702 targeting, and disseminations). Except as necessary to assess location under this provision, NSA may not use or disclose any information acquired pursuant to section 702 during such time period unless NSA determines, based on the totality of the circumstances, that the target is reasonably believed to have been located outside the United States at the time the information was acquired. If NSA determines that the target is reasonably believed to have been located inside the United States at the time the information was acquired, such information will not be used and will be promptly destroyed.

(U) Section 4 - Acquisition and Handling - Attorney-Client Communications

(U) As soon as it becomes apparent that a communication is between a person who is known to be under criminal indictment in the United States and an attorney who represents that individual in the matter under indictment (or someone acting on behalf of the attorney), monitoring of that communication will cease and the communication will be identified as an attorney-client communication in a log maintained for that purpose. The relevant portion of the communication containing that conversation will be segregated and the National Security Division of the Department of Justice will be notified so that appropriate procedures may be established to protect such communications from review or use in any criminal prosecution, while preserving foreign intelligence information contained therein. Additionally, all proposed dissemination of information constituting United States person attorney-client privileged communications must be reviewed by the NSA Office of General Counsel prior to dissemination.

(U) Section 5 - Domestic Communications

~~(TS//SI//NF)~~ A communication identified as a domestic communication (and, if applicable, the Internet transaction in which it is contained) will be promptly destroyed upon recognition unless the Director (or Acting Director) of NSA specifically determines, in writing and on a communication-by-communication basis, that the sender or intended recipient of the domestic communication had been properly targeted under section 702 of the Act, and the domestic communication satisfies one or more of the following conditions:

(1) ~~(TS//SI//NF)~~ such domestic communication is reasonably believed to contain significant foreign intelligence information. Such domestic communication (and, if applicable, the transaction in which it is contained) may be retained, handled, and disseminated in accordance with these procedures;

(2) ~~(TS//SI//NF)~~ such domestic communication does not contain foreign intelligence information but is reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed. Such domestic communication may be disseminated (including United States person identities) to appropriate Federal law enforcement authorities, in accordance with 50 U.S.C. §§ 1806(b) and 1825(c), Executive Order No. 12333, and, where applicable, the crimes reporting procedures

set out in the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document. Such domestic communication (and, if applicable, the transaction in which it is contained) may be retained by NSA for a reasonable period of time, not to exceed six months unless extended in writing by the Attorney General, to permit law enforcement agencies to determine whether access to original recordings of such communication is required for law enforcement purposes;

(3) ~~(TS//SI//NF)~~ such domestic communication is reasonably believed to contain technical data base information, as defined in Section 2(j), or information necessary to understand or assess a communications security vulnerability. Such domestic communication may be provided to the FBI and/or disseminated to other elements of the United States Government. Such domestic communication (and, if applicable, the transaction in which it is contained) may be retained for a period sufficient to allow a thorough exploitation and to permit access to data that is, or is reasonably believed likely to become, relevant to a current or future foreign intelligence requirement. Sufficient duration may vary with the nature of the exploitation.

a. (U//~~FOUO~~) In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis.

b. ~~(S//SI~~ [redacted] In the case of communications that are not enciphered or otherwise reasonably believed to contain secret meaning, sufficient duration is five years from expiration date of the certification authorizing the collection for telephony communications and Internet communications acquired by or with the assistance of the FBI from Internet Service Providers, and two years from expiration date of the certification authorizing the collection for Internet transactions acquired through NSA's upstream collection techniques, unless the Signal Intelligence Director, NSA, determines in writing that retention of a specific communication for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements; or

(4) (U//~~FOUO~~) such domestic communication contains information pertaining to an imminent threat of serious harm to life or property. Such information may be retained and disseminated to the extent reasonably necessary to counter such threat.

~~(S//NF)~~ Notwithstanding the above, if a domestic communication indicates that a target has entered the United States, NSA may promptly notify the FBI of that fact, as well as any information concerning the target's location that is contained in the communication. NSA may also use information derived from domestic communications for collection avoidance purposes, and may provide such information to the FBI and CIA for collection avoidance purposes. NSA may retain the communication from which such information is

derived but shall restrict the further use or dissemination of the communication by placing it on the Master Purge List (MPL).

(U) Section 6 - Foreign Communications of or Concerning United States Persons

(a) (U) Retention

(U) Foreign communications of or concerning United States persons collected in the course of an acquisition authorized under section 702 of the Act may be retained only:

(1) (U) if necessary for the maintenance of technical data bases. Retention for this purpose is permitted for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future foreign intelligence requirement. Sufficient duration may vary with the nature of the exploitation.

a. (U) In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis.

b. ~~(TS//SI//NF)~~ In the case of communications that are not enciphered or otherwise reasonably believed to contain secret meaning, sufficient duration is five years from expiration date of the certification authorizing the collection for telephony communications and Internet communications acquired by or with the assistance of the FBI from Internet Service Providers, and two years from expiration date of the certification authorizing the collection for Internet transactions acquired through NSA's upstream collection techniques, unless the Signals Intelligence Director, NSA, determines in writing that retention of a specific category of communications for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements;

(2) (U) if dissemination of such communications with reference to such United States persons would be permitted under subsection (b) below; or

(3) (U) if the information is evidence of a crime that has been, is being, or is about to be committed and is provided to appropriate federal law enforcement authorities.

~~(TS//SI//NF)~~ Foreign communications of or concerning United States persons that may be retained under subsections 6(a)(2) and (3) above include discrete communications contained in Internet transactions, provided that NSA has specifically determined, consistent with subsection 3(c)(2) above, that each discrete communication within the Internet transaction either: (a) is to, from, or about a tasked selector; or (b) is not to, from, or about a tasked selector and is also not to or from an identifiable United States person or person reasonably believed to be in the United States.

(b) (U) Dissemination

(U) A dissemination based on communications of or concerning a United States person may be made in accordance with Section 7 or 8 below if the identity of the United States person is deleted and a generic term or symbol is substituted so that the information cannot reasonably be connected with an identifiable United States person. Otherwise, dissemination of intelligence based on communications of or concerning a United States person may only be made to a recipient requiring the identity of such person for the performance of official duties but only if at least one of the following criteria is also met:

(1) (U) the United States person has consented to dissemination or the information of or concerning the United States person is available publicly;

(2) (U) the identity of the United States person is necessary to understand foreign intelligence information or assess its importance, e.g., the identity of a senior official in the Executive Branch;

(3) (U) the communication or information indicates that the United States person may be:

a. an agent of a foreign power;

b. a foreign power as defined in section 101(a) of the Act;

c. residing outside the United States and holding an official position in the government or military forces of a foreign power;

d. a corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or

e. acting in collaboration with an intelligence or security service of a foreign power and the United States person has, or has had, access to classified national security information or material;

(4) (U) the communication or information indicates that the United States person may be the target of intelligence activities of a foreign power;

(5) (U) the communication or information indicates that the United States person is engaged in the unauthorized disclosure of classified national security information or the United States person's identity is necessary to understand or assess a communications or network security vulnerability, but only after the agency that originated the information certifies that it is properly classified;

(6) (U) the communication or information indicates that the United States person may be engaging in international terrorist activities;

(7) (U//~~FOUO~~) the acquisition of the United States person's communication was authorized by a court order issued pursuant to the Act and the communication may relate to the foreign intelligence purpose of the surveillance; or

(8) (U) the communication or information is reasonably believed to contain evidence that a crime has been, is being, or is about to be committed, provided that dissemination is for law enforcement purposes and is made in accordance with 50 U.S.C. §§ 1806(b) and 1825(c), Executive Order No. 12333, and, where applicable, the crimes reporting procedures set out in the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document.

(c) (U) Provision of Unminimized Communications to CIA and FBI

(1) (U) NSA may provide to the Central Intelligence Agency (CIA) unminimized communications acquired pursuant to section 702 of the Act. CIA will identify to NSA targets for which NSA may provide unminimized communications to CIA. CIA will handle any such unminimized communications received from NSA in accordance with CIA minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act.

(2) (U) NSA may provide to the FBI unminimized communications acquired pursuant to section 702 of the Act. The FBI will identify to NSA targets for which NSA may provide unminimized communications to the FBI. The FBI will handle any such unminimized communications received from NSA in accordance with FBI minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act.

(U) Section 7 - Other Foreign Communications

(U) Foreign communications of or concerning a non-United States person may be retained, used, and disseminated in any form in accordance with other applicable law, regulation, and policy.

(~~TS//SI//NF~~) Foreign communications of or concerning a non-United States person that may be retained under this subsection include discrete communications contained in Internet transactions, provided that NSA has specifically determined, consistent with subsection 3(c)(2) above, that each discrete communication within the Internet transaction either: (a) is to, from, or about a tasked selector; or (b) is not to, from, or about a tasked selector and is also not to or from an identifiable United States person or person reasonably believed to be in the United States.

(U//~~FOUO~~) Additionally, foreign communications of or concerning a non-United States person may be retained for the same purposes and in the same manner as detailed in Section 6(a)(1), above.

(U) Section 8 - Collaboration with Foreign Governments

(a) (U) Procedures for the dissemination of evaluated and minimized information. Pursuant to section 1.7(c)(8) of Executive Order No. 12333, as amended, NSA conducts foreign cryptologic liaison relationships with certain foreign governments. Information acquired pursuant to section 702 of the Act may be disseminated to a foreign government. Except as provided below in subsection 8(b) of these procedures, any dissemination to a foreign government of information of or concerning a United States person that is acquired pursuant to section 702 may only be done in a manner consistent with sections 6(b) and 7 of these NSA minimization procedures.

(b) (U) Procedures for technical or linguistic assistance. It is anticipated that NSA may obtain information or communications that, because of their technical or linguistic content, may require further analysis by foreign governments to assist NSA in determining their meaning or significance. Notwithstanding other provisions of these minimization procedures, NSA may disseminate computer disks, tape recordings, transcripts, or other information or items containing unminimized information or communications acquired pursuant to section 702 to foreign governments for further processing and analysis, under the following restrictions with respect to any materials so disseminated:

(1) (U) Dissemination to foreign governments will be solely for translation or analysis of such information or communications, and assisting foreign governments will make no use of any information or any communication of or concerning any person except to provide technical and linguistic assistance to NSA.

(2) (U) Dissemination will be only to those personnel within foreign governments involved in the translation or analysis of such information or communications. The number of such personnel will be restricted to the extent feasible. There will be no dissemination within foreign governments of this unminimized data.

(3) (U) Foreign governments will make no permanent agency record of information or communications of or concerning any person referred to or recorded on computer disks, tape recordings, transcripts, or other items disseminated by NSA to foreign governments, provided that foreign governments may maintain such temporary records as are necessary to enable them to assist NSA with the translation or analysis of such information. Records maintained by foreign governments for this purpose may not be disseminated within the foreign governments, except to personnel involved in providing technical or linguistic assistance to NSA.

(4) (U) Upon the conclusion of such technical or linguistic assistance to NSA, computer disks, tape recordings, transcripts, or other items or information disseminated to foreign governments will either be returned to NSA or be destroyed with an accounting of such destruction made to NSA.

(5) (U) Any information that foreign governments provide to NSA as a result of such technical or linguistic assistance may be disseminated by NSA in accordance with these minimization procedures.

7/24/14
Date

Eric H. Holder, Jr.
Attorney General of the United States

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix I

What do parrots and BGP routers have in common?

David Hauweele*, Bruno Quoitin
University of Mons (UMONS)
{first.last}@umons.ac.be

Cristel Pelsser†
University of Strasbourg
pelsser@unistra.fr

Randy Bush
Internet Initiative Japan (IIJ)
randy@psg.com

ABSTRACT

The Border Gateway Protocol propagates routing information accross the Internet in an incremental manner. It only advertises to its peers changes in routing. However, as early as 1998, observations have been made of BGP announcing the same route multiple times, causing router CPU load, memory usage and convergence time higher than expected.

In this paper, by performing controlled experiments, we pinpoint multiple causes of duplicates, ranging from the lack of full RIB-Outs to the discrete processing of update messages. To mitigate these duplicates, we insert a cache at the output of the routers. We test it on public BGP traces and discuss the relation of the cache performance with the existence of bursts of updates in the trace.

1. INTRODUCTION

The Border Gateway Protocol [1] (BGP) is the de facto standard used to exchange inter-AS routing information on the Internet. Its correct and scalable behavior is critical to the operation of the Internet. One of the keys to BGP scalability is the use of *incremental routing updates*: only changes in destination prefix reachability are advertised. These changes include the reachability of a new prefix, the unreachability of an existing destination (withdrawal), or a modification of the path attributes associated with a destination. Path attributes are involved in routing decisions and also ensure proper protocol behavior such as avoiding routing loops. According to the protocol specification, a BGP speaker should not issue an update containing the same BGP information as was most recently advertised for the prefix.

Anomalous BGP behavior has been observed as early as 1998 [2]. Based on a 9 months trace of the BGP traffic exchanged between backbone networks, Labovitz et al. showed lack of aggregation and high routing instability with up to 99% of exchanged routing information not being related to topological changes. In particular, they observed the occurrence of redundant BGP update messages that they called *duplicate updates*. At that time, most of the duplicates where due to bogus stateless BGP implementations. The authors noted that the observed high level of instability was detrimental to the operations of the Internet, causing high router CPU load, making routers unresponsive and in the worst cases leading to packet or routing information losses. In addition, they may sometimes trigger unreachability when interacting with route flap damping [3].

Several studies later revisited BGP dynamics [4–8] and its impact on router CPU load [9], some focused on BGP duplicates. Although the number of pathological updates declined over time, duplicates still constitute a significant part of the BGP traffic with up to 15% of the updates observed at RIPE monitors in 2006 [5]. It was later shown that the duplicate problem is even worse for routers in the core of the Internet with the portion of duplicates varying from 7% to 60% in 2008 [7]. More recently, in 2009, Park et al. [6] studied over 90 RouteViews/RIPE monitors and showed that the duplicates make up 13.5% of the aggregated BGP traffic. Routers can receive up to 86.4% of duplicates during their busiest time. These previous works show that duplicates are a continuing problem. We confirm this observation by looking at all sessions from EQUINIX, ISC, LINX and WIDE RouteViews collectors from 2009 to 2014. 48.5% of the traces we observed had more than 10% of duplicates. The traces also display a high variability with an average of $(18.84 \pm 22.31)\%$ duplicates. Finally, [6] hinted that a change in attributes attached to iBGP routes may trigger eBGP duplicates. To the best of our knowledge, so far, no thorough study has explained their origin or tried to mitigate the problem.

In this paper, we make the following contributions:

- We discuss in Section 2 the causes of today's duplicates. Although the majority of duplicates in 1998 were bogus route withdrawals, this is not the case today (less than 0.5% on almost all traces). To understand what causes duplicates, we inject carefully crafted BGP updates into a router and we correlate the input and output BGP traffic. Based on this, we identify different causes for duplicates. Most duplicates today are due to implementions trading off between memory footprint and statefulness.

- In Section 3, we devise a caching mechanism that mitigates duplicates. The benefit of using a cache is that the amount of memory used can be controlled. We evaluate the efficiency of our caching mechanism on several real world BGP traces, using several replacement strategies. We show that our cache significantly reduces duplicates for prefixes in the default free zone even with a small cache size.

2. THE ORIGIN OF DUPLICATES

To investigate the origin of BGP duplicates, we follow two different approaches. First we look at a router that receives live BGP feeds. We capture all the BGP traffic and we man-

*David started this work during his internship at IIJ.

†The credits go to IIJ for supporting Cristel's work.

ually correlate duplicates observed in the outbound traffic with messages in the inbound traffic. This is an approach similar to that used by Park et al. in [6] that gives us some initial insight on potential causes for duplicates.

Second, we perform a fully controlled experiment where we inject crafted sequences of messages into a test router. We then look for duplicates in the output messages. Our experiment allows to confirm the hypotheses of Park et al. on the origin of duplicates. We also go much further as we establish three additional causes for duplicates.

This section explains our methodology and subsequent observations.

2.1 Definitions

We define a duplicate as a *redundant* prefix advertisement with the *same attributes* as the most recent update for this prefix on the same session and not interleaved with a withdrawal or a session reset. This definition is stricter than the one in [2] where an update is considered a duplicate (AADup) if its AS-Path and Next-Hop do not change. When we count duplicates, we include the initial duplicated route advertisement.

We also define the *ratio of duplicates* as the number of duplicates (including the original messages) over the total number of messages. With this definition, a trace where every advertisement is duplicated will have a ratio of 100%.

2.2 Real BGP feed experiment

The objective of this experiment is to manually investigate some occurrences of duplicates by correlating the duplicates observed at the output of a router with the messages it receives. Our setup is shown in Fig. 1. Devices $r0$, $r1$ (Cisco) and $r2$ (Juniper) are real routers while *mon*0 is a dedicated host running a software BGP router (Quagga).

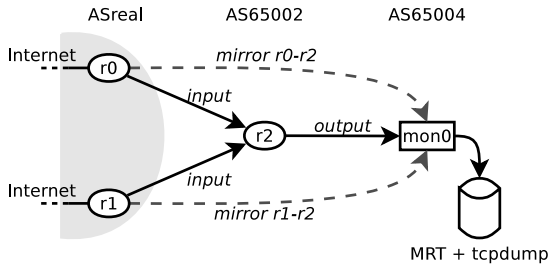


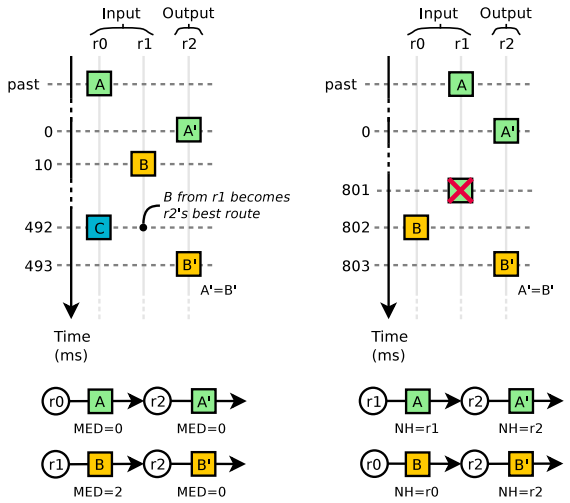
Figure 1: Setup for the I/O correlation.

The router under test is $r2$. It receives BGP messages from $r0$ and $r1$ through *input* eBGP sessions. After selecting its best routes, $r2$ sends BGP messages over a single *output* eBGP session to *mon*0. The routes learned by $r0$ and $r1$ are from real BGP feeds received in September 2013 for a duration of 23 days.

The *mon*0 host captures all the BGP messages received on the *mirror* and *output* sessions. The *mirror* sessions (dashed lines on Fig. 1) allow to capture the *input* routes advertised by the upstream routers $r0$ and $r1$. To reduce timing differences between the *input* and *mirror* sessions, both sessions are placed in the same update group on $r0$ and $r1$. The *Minimum Route Advertisement Interval* (MRAI) is also set to zero on these routers.

The messages are stored in MRT format. MRT records route advertisements, route changes and route withdrawals. Each record contains a timestamp and the path attributes. TCP-level traces of all the BGP messages received are also captured. This allows us to validate the MRT capture and dwelve deeper in the BGP message packet details e.g. to check the ordering of attributes.

We describe in the following paragraphs two common cases we observed. The first case involves the Multi-Exit-Discriminator (MED) attribute while the second case involves a rewritten Next-Hop. We do not know the exact frequency of these cases, as we have to manually extract the data.



(a) MED case (b) Next-Hop case

Figure 2: Common causes of duplicates. Timeline of the updates seen at the output of each router.

In the MED case, illustrated in Fig. 2a, we believe the duplicate is caused by a MED attribute stripped at the output of $r2$. Three different *input* routes are involved, all for the same IPv4 prefix. The first route, A, has an AS-Path of length 5 and a MED value of 0. The second route, B, has the same AS Path as A but a MED value of 2. The third route, C, has an AS Path of length 6 and a MED value of 0. At time 0ms, $r2$ announces route A learned from $r0$. Before announcing A, $r2$ updates the AS-Path and strips the MED, which produces route A'. At time 10ms, $r1$ announces route B to $r2$. The decision process of $r2$ ranks route A better than route B, causing no change in $r2$'s best route. At time 492ms, $r0$ announces to $r2$ route C which has a longer AS-Path. Route C implicitly withdraws route A. As a consequence, $r2$ now selects route B as best. Before announcing B, $r2$ strips the MED value, producing B'. *Output* routes A' and B' are equal, hence B' is a duplicate of A'.

In the case illustrated in Fig. 2b, we believe the duplicate is caused by the next-hop attribute. This case involves two routes. Route A announced first by router $r1$, is selected as best by $r2$ and announced on the *output* session at time 0ms. Before announcing route A, $r2$ rewrites the next-hop and emits route A'. At time 801ms, router $r1$ explicitly withdraws route A. At time 802ms, router $r0$ announces route B although it does not trigger any change in $r2$ yet. Finally, at time 803ms, router $r2$ selects route B as best. Before announcing route B, $r2$ rewrites the next-hop value with its own IP address, leading to route B'. Routes A and B only differ by their next-hop (resp. $r1$ and $r0$), hence routes A' and B' are identical.

2.3 Controlled experiment

To confirm the hypotheses of the previous section, we perform the same input/output matching in a fully controlled experiment. We systematically test a large set of situations that may not have appeared in the setting with a real, live BGP feed. We are able to find additional causes of duplicates and pinpoint more precisely the reasons behind these duplicates.

The setup depicted in Fig. 3 is similar to the previous experiment except we use a machine *inj*0, running Linux, to inject crafted updates to the router under test, *r*0, and another to capture its *output*. Router *r*0 is a Cisco 7200 running IOS v15.3. On *inj*0, we use ExaBGP [10] to inject synthetic updates. The monitoring host *mon*0 collects the routes observed on the *output* and *mirror* sessions with a Quagga BGP daemon and with tcpdump. The *mirror* session is used to validate *inj*0's program. We check the ability of this program to send BGP messages accurately. We measure that the minimum interval between two consecutive updates sent by ExaBGP is 1ms.

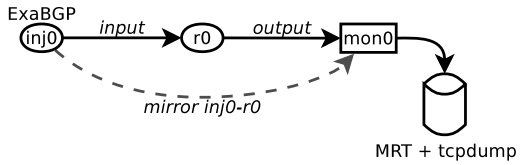


Figure 3: Setup for the injection.

Table 1 summarizes the results of the injection experiment. Due to space limitations, only results for a small number of test cases are presented. For each experiment, the first column shows the average delay between messages observed on the *input* and its standard deviation. Second column shows the same information for the *output*. The last column shows the ratio of duplicates. That is, the number of duplicates including the initial update over the number of updates (see Section 2.1).

Test case	Input (ms)	Output (ms)	Dup.
`NotVisible`	–	–	100%
`RFlap` (1 ms)	1.23 ± 0.50	3.47 ± 3.46	69.0%
`RFlap` (2 ms)	2.07 ± 0.39	2.84 ± 0.99	25.9%
`RFlap` (3 ms)	3.07 ± 0.44	3.06 ± 0.48	0.1%
`AFlap` (1 ms)	1.22 ± 0.69	3.74 ± 17.25	95.1%
`AFlap` (2 ms)	2.07 ± 0.36	2.07 ± 0.10	4.7%
`AFlap` (3 ms)	3.07 ± 0.44	3.06 ± 0.09	0.1%

Table 1: Results of selected injection test cases.

2.3.1 *Internal / non-transitive / filtered attributes*

This first set of experiments (`NotVisible`) considers the case of attributes whose changes should not be visible from the outside of an AS as they are either internal, non-transitive or filtered/rewritten by output policies. The objective of these experiments is to test whether or not such attributes could cause duplicate routes to be sent by the router.

For this purpose, we repeatedly send a sequence of 2 route updates (A, B) for the same destination prefix. Route B differs from route A for only a specific internal / non-transitive / filtered attribute. The expected behavior is as follows. When route A is received, it is selected as best as there is no other choice. It is then propagated on the output session. When route B is received, it replaces route A (implicit withdraw). Route B should not be propagated to the *output* session as it differs from route A only by an attribute that is either internal, non-transitive, or removed by a filter. Hence, on the *output* session, routes A and B are identical.

We observe a duplicate ratio of 100% for experiments in this class, as shown in Table 1 for the `NotVisible` test case. The router was not able to detect that the second route was a duplicate of the previous. We explain this behavior on the statelessness of the BGP implementation.

These results held for the following attributes: MED, Local Pref, Cluster List, and Originator ID. We also observed a 100% duplicates ratio for non-transitive Community values, for Community values stripped by outgoing policies and for rewritten Next-Hop (as already observed in Section 2.2).

2.3.2 *Fast flapping route*

In a second set of experiments (`RFlap`) we investigate the impact of a flapping route on the generation of duplicates. The experiment relies on the repetition of a simple sequence of 2 BGP updates (A, W) for the same prefix. A announces a route while W withdraws it.

The objective of this experiment is to trigger duplicates by forcing a route to change multiple times before the router has the opportunity to propagate it. To understand this behavior, we need to refine our model of how a router generates updates. When a route towards a prefix changes, the main BGP process does not send an update immediately. Instead, this task is delegated to a separate thread that periodically reads the RIB and advertises the routes marked as changed.

The following scenario illustrates how the transmission of a duplicate update can be caused. When the first Announce is received, the route is marked as changed in the RIB. The RIB is then scanned and an update is sent. Then, the Withdraw is received and the route is again marked as changed. However, before the RIB is scanned, the third message (second Announce) is received and the route is again marked as changed. When the RIB is scanned, the second Announce, identical to the first one is sent. It is a duplicate as the router did not have time to send a Withdraw between the two Announces.

We repeat this experiment with increasing delay between updates: 1ms, 2ms and 3ms. The results are in Table 1 for test case `RFlap`. We observe that with a 1ms interval, almost 70% of output updates are duplicates. When the interval between input updates increases, the ratio of duplicates decreases. With a 2ms interval, the ratio is almost 26% and at 3ms, there are almost no duplicates.

We also tested the impact of the MRAI on the generation of duplicates. We conducted the same experiment with a larger interval of 2 seconds and a MRAI set to 6 seconds. With this experiment we still generated more than 30% of duplicates.

2.3.3 *Flapping attribute*

This third set of experiments (`AFlap`) looks at flapping attributes. The principle is identical to the *RFlap* experiment except that the second message is not a withdraw but an update with a transitive attribute that flaps from one value to another and back. As an example, we present the results for routes where the origin AS in the AS-Path has value x in the first and third updates and has value $y \neq x$ in the sec-

ond update. We see in Table 1 for the `AFlap` test cases that the ratio of duplicates decreases with an increasing interval between the *input* BGP messages.

The explanation for these results is analogous to the *RFlap* experiment. When the interval between messages is small, the router marks the route as changed after the second message, but the third message, reversing the second update, is received before the second message is propagated downstream.

3. MITIGATING DUPLICATES

In Section 2, we found several causes explaining the generation of duplicates. According to the BGP specification, such duplicates should not appear. When a router advertises a route for a given prefix, it should store this route in the RIB-Out associated with the peer. When it later advertises a route for the same prefix, it looks at the current entry in the RIB-Out. If the current entry is the same as the new advertisement, the router does not send it because it would be a duplicate update.

We found out that although most router implementations support a RIB-Out, the implementation might be partial or operators might disable it to spare memory, especially on older hardware. Some vendors [11] explicitly recommend to disable the RIB-Out when the router has a large number of peers.

For this reason, we need to devise a solution that is not a full RIB-out but that still significantly reduces the number of BGP duplicates. This new mechanism must come at a lower cost than a RIB-Out in terms of memory consumption.

To obtain a baseline on the possible load reduction, we count the legitimate updates after filtering all duplicates. We compare this count to the number of updates in the original trace. We use a BGP trace obtained from the Equinix RouteViews collector and focus on the session with peer AS5769 (EQUIX-1). Fig. 4 shows two 12 hours excerpts of this session starting on 2013-9-17 at 0:00 (left) and 2013-9-18 at 4:00 (right). The Figure shows the total amount of updates received during the last hour (dark gray) and the same information after all duplicates have been filtered (light gray). On the left the trace has a relatively low rate of duplicates. We observe an average of 5,188 duplicates per hour. By filtering all duplicates, the number of updates on this period is reduced by an average factor of 1.62. On the right the trace features two large spikes of updates. On the largest spike, we count $5.46 * 10^5$ duplicates. By filtering all duplicates, the number of updates in this spike is reduced by a factor of 5.08.

We observe that a significant reduction in BGP traffic can be achieved by filtering duplicate updates. If CPU usage is proportional to the number of updates, sizable improvement in performance can be expected by getting rid of duplicates especially on small routers with limited CPU.

3.1 Caching router

Instead of a RIB-Out, we propose a small cache at the output of the router which can significantly reduce the number of duplicates at a far less memory cost. The advantage of this solution is that it can easily be added to the output of a router with little modifications of the BGP implementation.

A cache at the output of the router works similarly to a RIB-Out but using less memory. When a cache reaches its maximum capacity, it must remove one of its entries to add

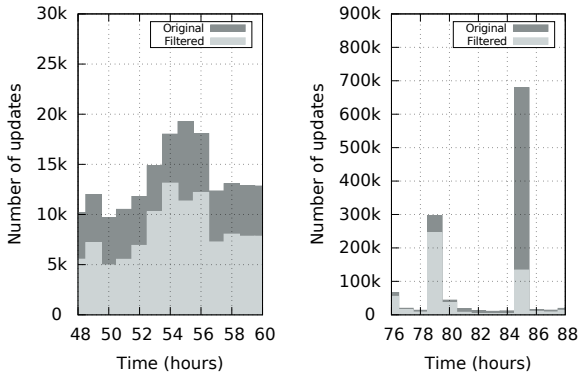


Figure 4: Two excerpts of the EQUIX-1 trace. Low rate of duplicates on the left. Spikes of duplicates on the right. We compare the original trace to the same trace with all duplicates filtered.

Name	Eviction strategy
`lru` / `mru`	Least/most recently queried entry.
`lrh` / `mrh`	Least/most recently hit entry.
`lfu` / `mfu`	Least/most frequently queried entry.
`lfh` / `mfh`	Least/most frequently hit entry.
`random`	Random entry.

Table 2: Eviction strategies

a new prefix. There are multiple ways to choose which prefix to remove when the cache is full. These selection methods are called *eviction strategies*. A cache is defined by its size and its eviction strategy.

In our case, the cache can be viewed as an Abstract Data Type (ADT) with the following operations: `query`, `remove` and `clear`. The `query` operation tells if an entry for a given key and value exists. If the given value is different from the entry in the cache, the entry is updated. If the cache does not contain an entry for this key, it adds this new entry to the cache. When the size reaches the cache limit, the cache eviction strategy comes into play. An entry is removed before the addition of the new entry to the cache. These two cases are considered *miss* queries. Instead, if the cache contains an entry for this key with the same value, the query is considered a *hit*.

The `remove` operation takes a key and if it exists, removes the associated entry from the cache. The `clear` operation removes all entries from the cache.

When the router advertises a given prefix and set of attributes, it queries the cache with the prefix as the key and the set of attributes as the value. In the case of a hit, the advertisement is a duplicate caught by the cache, and the router inhibits the advertisement. In the case of a miss, an advertisement is sent to the peer. When the router withdraws a given prefix, it removes the cache entry with the prefix as key and sends the withdraw to the peer. Finally when the router opens or reopens a session, the cache content is cleared and the router sends an open message to the peer.

3.2 Evaluation methodology

We assess the performance of the cache with the different eviction strategies listed in Table 2. The `random` cache

uses a pseudo random number generator to select an entry to remove. We use this strategy as a baseline to determine if other strategies are able to exploit characteristics of the input trace or if there is no specific pattern to exploit. Any such strategy should perform better in average than the random strategy.

In order to test the performance of the cache, we replay through the cache a previously captured trace. The cache then filters the duplicates. Since time does not matter for the eviction strategy, the cache can replay the trace without taking into account the elapsed time between each message. As a result it is possible to simulate the behavior of the cache on a captured trace much more rapidly than playing it directly on a router.

We use the Minimum Collection Time [12] (MCT) algorithm to accurately identify the start and duration of the routing table transfers in the BGP trace. We add an implicit OPEN message at the beginning of each detected table transfer so that updates within the table transfer do not count as duplicates.

3.3 Dataset

We measured the updates rate and duplicates ratio of several sessions at the RouteViews collectors from 2009 to 2014. We observed that the duplicate ratio was higher than 10% on 48.5% of the traces. The quantity of updates and duplicates also varies greatly from one session to another. The average rate of updates and duplicates per week across all traces observed in 2014 is of (3.6 ± 10.8) millions updates and (1.0 ± 3.7) millions duplicates respectively.

In order to take this variability into account, we apply the cache on three different sessions obtained from RouteViews collectors during one week period. We choose these three sessions as they contain a significant number of updates (> 1 million/week) but exhibit 3 extreme behaviours for what concerns the duplicates. Fig. 5 shows the hourly number of duplicates over time for these three traces.

	EQUIX-1	EQUIX-2	WIDE
Peer ASN	5769	2914	7500
Start	2013-09-15	2014-10-15	2013-09-15
End	2013-09-22	2014-10-22	2013-09-22
Updates	$4.5 * 10^6$	$1.55 * 10^7$	$1.2 * 10^6$
Duplicates	59.38%	98.36%	2.17%
Spikes	Large	No	Small

Table 3: Characteristics of three different traces.

Table 3 summarizes the characteristics of the traces. The number of updates and the ratio of duplicates observed vary greatly from one trace to another. The first trace, EQUIX-1, exhibits a large number of updates ($4.5{*}10^6$) and a high ratio of duplicates (59.38%), a large fraction of which (41%) visible as two large spikes of duplicates. In comparison EQUIX-2 has a higher number of updates ($1.55 * 10^7$) and a higher ratio of duplicates (98.36%) but displays no major spike. Finally the WIDE trace has a very low ratio of duplicates ($1.2 * 10^6$) and does not contain any large spike.

3.4 Results

We apply the cache on the WIDE and EQUIX-1 traces presented in Section 3.3. We also apply the cache on the third trace, EQUIX-2 with a fixed size of 65k entries and

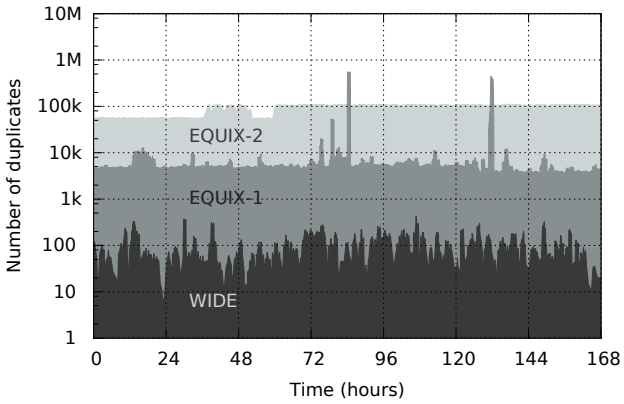


Figure 5: Three traces with different duplicates ratio. Each point shows the number of duplicates seen during the last hour.

Cache	WIDE 32k	WIDE 65k	EQUIX-1 32k	EQUIX-1 65k
No cache	2.172%		59.38%	
`lfh`	1.351%	0.885%	49.14%	45.50%
`lfu`	1.324%	0.818%	49.09%	45.45%
`lrh`	0.040%	**0.009%**	42.91%	42.27%
`lru`	**0.039%**	0.016%	**42.90%**	42.25%
`mfh`	1.556%	1.121%	53.85%	50.30%
`mfu`	0.830%	0.173%	52.97%	48.17%
`mrh`	1.555%	1.078%	53.34%	49.68%
`mfu`	1.518%	1.014%	52.93%	49.04%
`random`	0.042%	0.020%	42.98%	**41.87%**

Table 4: Percentage of duplicates at the output of the EQUIX-1 and WIDE traces for different cache eviction strategies and sizes expressed in number of different routes.

the `lru` strategy. These traces were captured at different locations and time. They show different behaviours against which we test our solution.

Table 4 summarizes the percentage of duplicates found at the output of the WIDE and EQUIX-1 traces for two cache sizes, 32768 (32k) and 65536 (65k) different routes, and multiple strategies. The first line gives the duplicate ratio of the original trace (no cache applied). For the WIDE trace, the `lru` and `lrh` eviction strategies provide the best results. The best cache, `lrh`, reduces the original duplicate ratio by a factor 241. Further, the larger cache provides better results. In the case of the WIDE trace, the `lru` cache is 2.44 times as effective in filtering the duplicates with a cache that is twice as large.

On the EQUIX-1 trace, the cache performs poorly. With a 32k cache, the best results are achieved with the `lru` strategy. However, the output duplicate ratio remains high, at 42.9%. Doubling the cache size does not provide as much benefit as with the WIDE trace. Moreover, a striking result is that in the case of the large cache, the `random` eviction performs better than the other techniques. This indicates that the eviction strategies are not able to properly exploit the characteristics of the trace.

These results suggest that a higher duplicate ratio inhibits the performance of the cache. However, when we apply the `lru` cache of 65k on the EQUIX-2 trace, which exhibits a

higher duplicates ratio than EQUIX-1, the duplicate ratio drops from 98.36% to 5.83%. This reduces the number of updates for the trace by a factor of 50.

This shows that a cache is able to filter a session with a very high number of duplicates. I.e., the performance does not depend on the number of duplicates but rather on other characteristics of the trace. Actually, it depends on the number of distinct prefixes at the origin of those duplicates. During the EQUIX-2 trace this number stays at an average of 1000 prefixes per hour. During the EQUIX-1 trace this number stays at the same value most of the time. However when the largest spike of duplicates occurs more than $2*10^5$ distinct prefixes are involved during less than one hour. As a result the cache did not retain most of the route changes occurring during this period. Hence subsequent duplicates caused by these routes were not filtered by the cache.

3.5 Discussion

Although a cache is effective in filtering feeds with a high ratio of duplicates (e.g. EQUIX-2), we observed that spikes of updates involving a large number of distinct prefixes are detrimental to the performance of the cache. These spikes can have multiple origins. First, spikes of updates can be caused by large routing events beyond the router. Second, spikes can be caused by routing table transfers following a session reset or a change in outbound policies. It is indeed common for network operators to prompt a table transfer with a ROUTE REFRESH message in order to apply changes in their inbound policies. However spikes in this second category must have been filtered by the MCT algorithm applied beforehand.

While we can explain the origin of spikes, we do not know if these spikes represent a frequent feature of the BGP sessions. We now measure the maximum spike size in term of distinct prefixes for all RouteViews sessions we observed during the year 2014. We also apply a `lru` cache of 65k entries on all these traces to map the performance of the cache to the size of the spikes observed in the sessions. The sample size for all measured sessions is of 1339 traces.

We define attenuation as the ratio of the number of duplicates seen in the original trace over the number of duplicates seen after the cache. The average attenuation of duplicates for all observed traces is 300.47. If we distinguish the traces by the size of their maximum spikes, the average attenuation for traces with spikes larger and smaller than the size of the cache are 1.26 and 370.06 respectively.

The existence of updates spikes can negatively impact the possibility to mitigate the duplicates. We measured the presence of spikes among all observed sessions in 2014. For this purpose, we consider there is a spike in a trace when more than 65k distinct prefixes at the origin of future duplicates are transferred in less than one hour. According to this definition, 11.73% of the traces displayed large spikes of duplicates.

4. CONCLUSION

Redundant consecutive BGP announcements consume unnecessary bandwidth and CPU in routers. In addition, these messages delay the propagation of useful routing information. We observed that BGP sessions exhibit different behaviors. For some session the number of duplicates is low. But other sessions can exhibit a very high ratio of duplicates. We identified large spikes of duplicates in 11.73% of the sessions we observed in 2014. This may be a problem on chatty sessions.

We then identified three causes of duplicates: changes in attributes that are not propagated further, flapping of routes or attributes and, finally, incorrect implementations for sets in AS-Paths. We verified these causes by performing thorough controlled experiments.

To mitigate the problem we propose use of a cache to find the right trade-off between additional memory consumption and the reduction of duplicates. We show that the performance of a cache highly depends on the characteristics of the BGP trace, in addition to the eviction strategy. While a cache is suitable on some traces, it is not always the case. The current trend of pushing control functions outside the router, to devices that are not as limited memory-wise, opens the door to full Adj-RIB-Outs and thus enable to avoid using pretty hacks to get rid of BGP duplicates completely in the future.

5. REFERENCES

[1] Y. Rekhter, T. Li, and S. Hares, "A Border Gateway Protocol 4 (BGP-4)," RFC 4271, Jan. 2006.

[2] C. Labovitz, G. R. Malan, and F. Jahanian, "Internet routing instability," *IEEE/ACM Transactions on Networking*, vol. 6, no. 5, pp. 515–528, 1998.

[3] C. Pelsser, O. Maennel, P. Mohapatra, R. Bush, and K. Patel, "Route flap damping made usable," in *Passive and Active Measurement*, 2011, pp. 143–152.

[4] C. Labovitz, A. Ahuja, A. Bose, and F. Jahanian, "Delayed internet routing convergence," *ACM SIGCOMM CCR*, vol. 30, no. 4, pp. 175–187, 2000.

[5] J. Li, M. Guidero, Z. Wu, E. Purpus, and T. Ehrenkranz, "BGP routing dynamics revisited," *ACM SIGCOMM CCR*, vol. 37, no. 2, pp. 5–16, 2007.

[6] J. H. Park, D. Jen, M. Lad, S. Amante, D. McPherson, and L. Zhang, "Investigating occurrence of duplicate updates in BGP announcements," in *Passive and Active Measurement*, 2010, pp. 11–20.

[7] A. Elmokashfi, A. Kvalbein, and C. Dovrolis, "BGP churn evolution: a perspective from the core," *IEEE/ACM Transactions on Networking*, vol. 20, no. 2, pp. 571–584, 2012.

[8] A. Elmokashfi and A. Dhamdhere, "Revisiting bgp churn growth," *ACM SIGCOMM CCR*, vol. 44, no. 1, pp. 5–12, Dec. 2013.

[9] S. Agarwal, C. Chuah, S. Bhattacharyya, and C. Diot, "Impact of BGP dynamics on router CPU utilization," in *Passive and Active Network Measurement*, 2004, pp. 278–288.

[10] "ExaBGP," http://github.com/Exa-Networks/exabgp, 2014.

[11] "EXOS," http://documentation.extremenetworks.com/exos_commands/EXOS_All/EXOS_Commands_All/r_disable-bgp-adjribout.shtml, 2015.

[12] P.-C. Cheng, B. Zhang, D. Massey, and L. Zhang, "Identifying BGP routing table transfers," *Computer Networks*, vol. 55, no. 3, pp. 636–649, 2011.

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix J

EXHIBIT A

Report on International Submarine Cables Landing in the US

Source: underlying data cloned from https://github.com/telegeography/www.submarinecablemap.com, most recent commit at 2018-01-02 14:09:33-05:00 (7d7cd9e8096d624717f2b4e56ebc72831e2ba7f6)

- US Landing Points for International Submarine Cables
- International Submarine Cables Landing in the US

US Landing Points for International Submarine Cables

Landing 1

Bandon, Oregon, United States

Location: (124.4°W, 43.12°N)

1 International Cable:

- FASTER

  Owners:
  Google, KDDI, SingTel, China Telecom, China Mobile, Global Transit
  Other Countries:
  Japan, Taiwan

Landing 2

Bellport, New York, United States

Location: (72.94°W, 40.76°N)

1 International Cable:

- Yellow

  Owners:
  Level 3
  Other Country:
  United Kingdom

Landing 3

Boca Raton, FL, United States

Location: (80.09°W, 26.35°N)

6 International Cables:

- South America-1 (SAm-1)

  Owners:
  Telxius
  Other Countries:
  Argentina, Brazil, Chile, Colombia, Dominican Republic, Ecuador, Guatemala, Peru

- Bahamas Internet Cable System (BICS)

  Owners:
  Caribbean Crossings
  Other Country:
  Bahamas

- Monet

  Owners:
  Angola Cables, Google, Algar Telecom, Antel Uruguay
  Other Country:
  Brazil

- Deep Blue Cable

  Owners:
  Deep Blue Cable
  Other Countries:
  Anguilla, Aruba, Bonaire, Sint Eustatius, and Saba, Cayman Islands, Colombia, Curaçao, Dominican Republic, Haiti, Jamaica, Panama, Saint Martin, Trinidad and Tobago, Turks and Caicos Islands

- GlobeNet

  Owners:
  BTG Pactual
  Other Countries:
  Bermuda, Brazil, Colombia, Venezuela

- Colombia-Florida Subsea Fiber (CFX-1)

  Owners:
  C&W Networks
  Other Countries:
  Colombia, Jamaica

Landing 4

Brookhaven, New York, United States

Location: (72.91°W, 40.77°N)

1 International Cable:

- Atlantic Crossing-1 (AC-1)

  Owners:
  Level 3
  Other Countries:
  Germany, Netherlands, United Kingdom

Landing 5

Buffalo, New York, United States

Location: (78.88°W, 42.89°N)

1 International Cable:

- Crosslake Fibre

  Owners:
  Crosslake Fibre
  Other Country:
  Canada

Landing 6

Charlestown, Rhode Island, United States

Location: (71.65°W, 41.41°N)

1 International Cable:

- Challenger Bermuda-1 (CB-1)

  Owners:
  Cable Co.
  Other Country:
  Bermuda

Landing 7

El Segundo, California, United States

Location: (118.4°W, 33.92°N)

1 International Cable:

- Pacific Light Cable Network (PLCN)

  Owners:
  Pacific Light Data Communication Co. Ltd., Google, Facebook
  Other Countries:
  China, Philippines, Taiwan

Landing 8

Grover Beach, California, United States

Location: (120.6°W, 35.12°N)

2 International Cables:

- Pan-American Crossing (PAC)

  Owners:
  Level 3
  Other Countries:
  Costa Rica, Mexico, Panama

- Pacific Crossing-1 (PC-1)

  Owners:
  NTT
  Other Country:
  Japan

Landing 9

Harbour Pointe, Washington, United States

Location: (122.3°W, 47.89°N)

1 International Cable:

- Pacific Crossing-1 (PC-1)

  Owners:
  NTT
  Other Country:
  Japan

Landing 10

Hermosa Beach, California, United States

Location: (118.4°W, 33.86°N)

2 International Cables:

- JUPITER

  Owners:
  Amazon, Facebook, NTT, PLDT, PCCW, Softbank Telecom
  Other Countries:
  Japan, Philippines

- SEA-US

  Owners:
  RTI, Inc., Globe Telecom, Hawaiian Telcom, GTA TeleGuam, Telin, Balau Submarine Cable Company, Federated States of Micronesia Telecommunications Company
  Other Countries:
  Federated States of Micronesia, Indonesia, Palau, Philippines

Landing 11

Hillsboro, Oregon, United States

Location: (123°W, 45.52°N)

2 International Cables:

- Southern Cross Cable Network (SCCN)

  Owners:
  Spark New Zealand, SingTel Optus, Verizon
  Other Countries:
  Australia, Fiji, New Zealand

- Tata TGN-Pacific

  Owners:
  Tata Communications
  Other Country:
  Japan

Landing 12 Hollywood, Florida, United States

Location: (80.16°W, 26.01°N)

4 International Cables:

- Columbus-III

  Owners:
  Telecom Italia Sparkle, AT&T, Verizon, Telefonica, Portugal Telecom, Tata Communications, Ukrtelecom, Telkom South Africa, Telecom Argentina, Instituto Costarricense de Electricidad, Embratel, Cyta
  Other Countries:
  Italy, Portugal, Spain

- America Movil Submarine Cable System-1 (AMX-1)

  Owners:
  América Móvil
  Other Countries:
  Brazil, Colombia, Dominican Republic, Guatemala, Mexico

- Americas-II

  Owners:
  Embratel, AT&T, Verizon, Sprint, CANTV, Tata Communications, Level 3, Telecom Argentina, Orange, Portugal Telecom, C&W Networks, Telecom Italia Sparkle, Entel Chile
  Other Countries:
  Brazil, Curaçao, French Guiana, Martinique, Trinidad and Tobago, Venezuela

- Maya-1

  Owners:
  Verizon, AT&T, Sprint, Hondutel, Telefonica, Orbitel, Telecom Italia Sparkle, C&W Networks, Entel Chile, Embratel, ETB, Axtel, Instituto Costarricense de Electricidad, Proximus, Prepa Networks, Orange, Tricom, RSL Telecom, América Móvil
  Other Countries:
  Cayman Islands, Colombia, Costa Rica, Honduras, Mexico, Panama

Landing 13

Island Park, New York, United States

Location: (73.66°W, 40.6°N)

1 International Cable:

- FLAG Atlantic-1 (FA-1)

  Owners:
  Global Cloud Xchange
  Other Countries:
  France, United Kingdom

Landing 14

Isla Verde, Puerto Rico, United States

Location: (66.02°W, 18.44°N)

3 International Cables:

- Saint Maarten Puerto Rico Network One (SMPR-1)

  Owners:
  TelEm Group, Dauphin Telecom
  Other Countries:
  Saint Martin, Sint Maarten

- ARCOS

  Owners:
  C&W Networks, CANTV, Codetel, Hondutel, Belize Telemedia, Enitel, AT&T, Alestra, Verizon, RACSA, United Telecommunication Services (UTS), Telecarrier, Tricom USA, Telecomunicaciones Ultramarinas de Puerto Rico, Internexa, Orbinet Overseas, Telepuerto San Isidro, Bahamas Telecommunications Company, Instituto Costarricense de Electricidad, Orbitel
  Other Countries:
  Bahamas, Belize, Colombia, Costa Rica, Curaçao, Dominican Republic, Guatemala, Honduras, Mexico, Nicaragua, Panama, Turks and Caicos Islands, Venezuela

- Antillas 1

  Owners:
  AT&T, Verizon, Sprint, Tata Communications, Orange, C&W Networks, Telecom Italia Sparkle, Embratel
  Other Country:
  Dominican Republic

Landing 15 Jacksonville, Florida, United States

Location: (81.66°W, 30.33°N)

3 International Cables:

- America Movil Submarine Cable System-1 (AMX-1)

  Owners:
  América Móvil
  Other Countries:
  Brazil, Colombia, Dominican Republic, Guatemala, Mexico

- South America Pacific Link (SAPL)

  Owners:
  Ocean Networks
  Other Countries:
  Chile, Panama

- Pacific Caribbean Cable System (PCCS)

  Owners:
  C&W Networks, Telconet, Setar, United Telecommunication Services (UTS), Telxius
  Other Countries:
  Aruba, Colombia, Curaçao, Ecuador, Panama

Landing 16 Kahe Point, Hawaii, United States

Location: (158.1°W, 21.35°N)

1 International Cable:

- Southern Cross Cable Network (SCCN)

  Owners:
  Spark New Zealand, SingTel Optus, Verizon
  Other Countries:
  Australia, Fiji, New Zealand

Landing 17

Kapolei, HI, United States

Location: (158.1°W, 21.34°N)

1 International Cable:

- Hawaiki

  Owners:
  Hawaiki Cable Company
  Other Countries:
  Australia, New Zealand

Landing 18

Kawaihae, Hawaii, United States

Location: (155.8°W, 20.04°N)

1 International Cable:

- Honotua

  Owners:
  OPT French Polynesia
  Other Country:
  French Polynesia

Landing 19

Keawaula, Hawaii, United States

Location: (158.2°W, 21.43°N)

2 International Cables:

- Telstra Endeavour

  Owners:
  Telstra
  Other Country:
  Australia

- Asia-America Gateway (AAG) Cable System

  Owners:
  Telekom Malaysia, AT&T, Starhub, PLDT, Communications Authority of Thailand, Airtel (Bharti), Telstra, Telkom Indonesia, BT, Eastern Telecom, PT Indonesia Satellite Corp., Spark New Zealand, Viettel Corporation, Saigon Postel Corporation, Vietnam Telecom International, Brunei International Gateway, BayanTel, Ezecom
  Other Countries:
  Brunei, China, Malaysia, Philippines, Singapore, Thailand, Vietnam

Landing 20

Los Angeles, California, United States

Location: (118.2°W, 34.05°N)

1 International Cable:

- Tata TGN-Pacific

  Owners:
  Tata Communications
  Other Country:
  Japan

Landing 21

Lynn, Massachusetts, United States

Location: (70.95°W, 42.46°N)

1 International Cable:

- GTT Atlantic

  Owners:
  GTT
  Other Countries:
  Canada, Ireland, United Kingdom

Landing 22

Makaha, Hawaii, United States

Location: (158.2°W, 21.46°N)

3 International Cables:

- Japan-U.S. Cable Network (JUS)

  Owners:
  Verizon, AT&T, BT, Sprint, CenturyLink, KDDI, NTT, Chunghwa Telecom, Tata Communications, SingTel, Telekom Malaysia, Softbank Telecom, Orange, Level 3, SK Broadband, KT, China Telecom, China Unicom, LG Uplus, HKBN Enterprise Solutions, Starhub, PCCW, Telstra, Vodafone, PLDT
  Other Country:
  Japan

- South America Pacific Link (SAPL)

  Owners:
  Ocean Networks
  Other Countries:
  Chile, Panama

- SEA-US

  Owners:
  RTI, Inc., Globe Telecom, Hawaiian Telcom, GTA TeleGuam, Telin, Balau Submarine Cable Company, Federated States of Micronesia Telecommunications Company
  Other Countries:
  Federated States of Micronesia, Indonesia, Palau, Philippines

Landing 23

Manasquan, New Jersey, United States

Location: (74.05°W, 40.12°N)

3 International Cables:

- TAT-14

  Owners:
  BT, Verizon, Deutsche Telekom, Orange, Sprint, TeliaSonera, Level 3, KPN, Telenor, Etisalat, OTEGLOBE, SingTel, KDDI, Softbank Telecom, Zayo Group, Portugal Telecom, Slovak Telekom, TDC, Telus, Tata Communications, Telefonica, AT&T, Proximus, Elisa Corporation, Cyta, Rostelecom, Vodafone
  Other Countries:
  Denmark, France, Germany, Netherlands, United Kingdom

- Gemini Bermuda

  Owners:
  C&W Networks
  Other Country:
  Bermuda

- Apollo

  Owners:
  Vodafone
  Other Countries:
  France, United Kingdom

Landing 24

Manchester, California, United States

Location: (123.7°W, 38.97°N)

1 International Cable:

- Japan-U.S. Cable Network (JUS)

  Owners:
  Verizon, AT&T, BT, Sprint, CenturyLink, KDDI, NTT, Chunghwa Telecom, Tata Communications, SingTel, Telekom Malaysia, Softbank Telecom, Orange, Level 3, SK Broadband, KT, China Telecom, China Unicom, LG Uplus, HKBN Enterprise Solutions, Starhub, PCCW, Telstra, Vodafone, PLDT
  Other Country:
  Japan

Landing 25

Miramar, Puerto Rico, United States

Location: (66.08°W, 18.45°N)

2 International Cables:

- Americas-II

  Owners:
  Embratel, AT&T, Verizon, Sprint, CANTV, Tata Communications, Level 3, Telecom Argentina, Orange, Portugal Telecom, C&W Networks, Telecom Italia Sparkle, Entel Chile
  Other Countries:
  Brazil, Curaçao, French Guiana, Martinique, Trinidad and Tobago, Venezuela

- Antillas 1

  Owners:
  AT&T, Verizon, Sprint, Tata Communications, Orange, C&W Networks, Telecom Italia Sparkle, Embratel
  Other Country:
  Dominican Republic

Landing 26

Morro Bay, California, United States

Location: (120.8°W, 35.37°N)

2 International Cables:

- Japan-U.S. Cable Network (JUS)

  Owners:
  Verizon, AT&T, BT, Sprint, CenturyLink, KDDI, NTT, Chunghwa Telecom, Tata Communications, SingTel, Telekom Malaysia, Softbank Telecom, Orange, Level 3, SK Broadband, KT, China Telecom, China Unicom, LG Uplus, HKBN Enterprise Solutions, Starhub, PCCW, Telstra, Vodafone, PLDT
  Other Country:
  Japan

- Southern Cross Cable Network (SCCN)

  Owners:
  Spark New Zealand, SingTel Optus, Verizon
  Other Countries:
  Australia, Fiji, New Zealand

Landing 27

Naples, FL, United States

Location: (81.8°W, 26.14°N)

1 International Cable:

- Deep Blue Cable

  Owners:
  Deep Blue Cable
  Other Countries:
  Anguilla, Aruba, Bonaire, Sint Eustatius, and Saba, Cayman Islands, Colombia, Curaçao, Dominican Republic, Haiti, Jamaica, Panama, Saint Martin, Trinidad and Tobago, Turks and Caicos Islands

Landing 28

Nedonna Beach, Oregon, United States

Location: (123.9°W, 45.64°N)

1 International Cable:

- Trans-Pacific Express (TPE) Cable System

  Owners:
  China Telecom, China Unicom, Chunghwa Telecom, KT, Verizon, NTT, AT&T
  Other Countries:
  China, Japan, Taiwan

Landing 29

North Miami Beach, Florida, United States

Location: (80.16°W, 25.93°N)

1 International Cable:

- ARCOS

  Owners:
  C&W Networks, CANTV, Codetel, Hondutel, Belize Telemedia, Enitel, AT&T, Alestra, Verizon, RACSA, United Telecommunication Services (UTS), Telecarrier, Tricom USA, Telecomunicaciones Ultramarinas de Puerto Rico, Internexa, Orbinet Overseas, Telepuerto San Isidro, Bahamas Telecommunications Company, Instituto Costarricense de Electricidad, Orbitel
  Other Countries:
  Bahamas, Belize, Colombia, Costa Rica, Curaçao, Dominican Republic, Guatemala, Honduras, Mexico, Nicaragua, Panama, Turks and Caicos Islands, Venezuela

Landing 30

Northport, New York, United States

Location: (73.34°W, 40.91°N)

1 International Cable:

- FLAG Atlantic-1 (FA-1)

  Owners:
  Global Cloud Xchange
  Other Countries:
  France, United Kingdom

Landing 31

Pacific City, OR, United States

Location: (124°W, 45.2°N)

2 International Cables:

- Hawaiki

  Owners:
  Hawaiki Cable Company
  Other Countries:
  Australia, New Zealand

- New Cross Pacific (NCP) Cable System

  Owners:
  China Telecom, China Unicom, Chunghwa Telecom, KT, China Mobile, Microsoft, Softbank Telecom
  Other Countries:
  China, Japan, Taiwan

Landing 32

Pago Pago, American Samoa

Location: (170.7°W, -14.28°N)

2 International Cables:

- Hawaiki

  Owners:
  Hawaiki Cable Company
  Other Countries:
  Australia, New Zealand

- Samoa-American Samoa (SAS)

  Owners:
  American Samoa Government, Elandia
  Other Country:
  Samoa

Landing 33 Piti, Guam

Location: (-144.7°W, 13.46°N)

5 International Cables:

- HANTRU1 Cable System

  Owners:
  Hannon Armstrong, Federated States of Micronesia Telecommunications Company, Marshall Islands Telecommunications Authority
  Other Country:
  Federated States of Micronesia

- PIPE Pacific Cable-1 (PPC-1)

  Owners:
  TPG
  Other Countries:
  Australia, Papua New Guinea

- Hong Kong-Guam (HK-G)

  Owners:
  RTI Connectivity
  Other Country:
  China

- Tata TGN-Pacific

  Owners:
  Tata Communications
  Other Country:
  Japan

- SEA-US

  Owners:
  RTI, Inc., Globe Telecom, Hawaiian Telcom, GTA TeleGuam, Telin, Balau Submarine Cable Company, Federated States of Micronesia Telecommunications Company
  Other Countries:
  Federated States of Micronesia, Indonesia, Palau, Philippines

Landing 34

Redondo Beach, California, United States

Location: (118.4°W, 33.84°N)

1 International Cable:

- Unity/EAC-Pacific

  Owners:
  Telstra, Google, Global Transit, SingTel, KDDI, Airtel (Bharti)
  Other Country:
  Japan

Landing 35

San Juan, Puerto Rico, United States

Location: (66.11°W, 18.47°N)

7 International Cables:

- America Movil Submarine Cable System-1 (AMX-1)

  Owners:
  América Móvil
  Other Countries:
  Brazil, Colombia, Dominican Republic, Guatemala, Mexico

- South America-1 (SAm-1)

  Owners:
  Telxius
  Other Countries:
  Argentina, Brazil, Chile, Colombia, Dominican Republic, Ecuador, Guatemala, Peru

- Deep Blue Cable

  Owners:
  Deep Blue Cable
  Other Countries:
  Anguilla, Aruba, Bonaire, Sint Eustatius, and Saba, Cayman Islands, Colombia, Curaçao, Dominican Republic, Haiti, Jamaica, Panama, Saint Martin, Trinidad and Tobago, Turks and Caicos Islands

- Global Caribbean Network (GCN)

  Owners:
  Leucadia National Corporation, Loret Group
  Other Country:
  Guadeloupe

- Pacific Caribbean Cable System (PCCS)

  Owners:
  C&W Networks, Telconet, Setar, United Telecommunication Services (UTS), Telxius
  Other Countries:
  Aruba, Colombia, Curaçao, Ecuador, Panama

- Southern Caribbean Fiber

  Owners:
  Digicel
  Other Countries:
  Antigua and Barbuda, Barbados, Dominica, Grenada, Guadeloupe, Martinique, Saint-Barthélemy, Saint Kitts and Nevis, Saint Lucia, Saint Martin, Saint Vincent and the Grenadines, Trinidad and Tobago

- BRUSA

  Owners:
  Telxius
  Other Country:
  Brazil

Landing 36 San Luis Obispo, California, United States

Location: (120.7°W, 35.29°N)

1 International Cable:

- Asia-America Gateway (AAG) Cable System

  Owners:
  Telekom Malaysia, AT&T, Starhub, PLDT, Communications Authority of Thailand, Airtel (Bharti), Telstra, Telkom Indonesia, BT, Eastern Telecom, PT Indonesia Satellite Corp., Spark New Zealand, Viettel Corporation, Saigon Postel Corporation, Vietnam Telecom International, Brunei International Gateway, BayanTel, Ezecom
  Other Countries:
  Brunei, China, Malaysia, Philippines, Singapore, Thailand, Vietnam

Landing 37 Sarasota, Florida, United States

Location: (82.54°W, 27.34°N)

1 International Cable:

- AURORA

  Owners:
  FP Telecommunications
  Other Countries:
  Belize, Chile, Colombia, Costa Rica, Ecuador, Guatemala, Honduras, Mexico, Nicaragua, Panama

Landing 38

Shirley, New York, United States

Location: (72.87°W, 40.8°N)

2 International Cables:

- AEConnect (AEC)

  Owners:
  Aqua Comms
  Other Country:
  Ireland

- Apollo

  Owners:
  Vodafone
  Other Countries:
  France, United Kingdom

Landing 39

Spanish River Park, Florida, United States

Location: (80.07°W, 26.38°N)

1 International Cable:

- Bahamas Internet Cable System (BICS)

  Owners:
  Caribbean Crossings
  Other Country:
  Bahamas

Landing 40

Spencer Beach, Hawaii, United States

Location: (155.8°W, 20.02°N)

1 International Cable:

- Southern Cross Cable Network (SCCN)

  Owners:
  Spark New Zealand, SingTel Optus, Verizon
  Other Countries:
  Australia, Fiji, New Zealand

Landing 41

St. Croix, Virgin Islands, United States

Location: (64.82°W, 17.77°N)

5 International Cables:

- South American Crossing (SAC)/Latin American Nautilus (LAN)

  Owners:
  Level 3, Telecom Italia Sparkle
  Other Countries:
  Argentina, Brazil, Chile, Colombia, Panama, Peru, Venezuela

- Americas-II

  Owners:
  Embratel, AT&T, Verizon, Sprint, CANTV, Tata Communications, Level 3, Telecom Argentina, Orange, Portugal Telecom, C&W Networks, Telecom Italia Sparkle, Entel Chile
  Other Countries:
  Brazil, Curaçao, French Guiana, Martinique, Trinidad and Tobago, Venezuela

- Pan American (PAN-AM)

  Owners:
  AT&T, Telefonica del Peru, Softbank Telecom, Telecom Italia Sparkle, Sprint, CANTV, Tata Communications, Telefónica de Argentina, Telstra, Verizon, Entel Chile, Telecom Argentina, Telconet, Instituto Costarricense de Electricidad, C&W Networks, Embratel
  Other Countries:
  Aruba, Chile, Colombia, Ecuador, Panama, Peru, Venezuela

- Global Caribbean Network (GCN)

  Owners:
  Leucadia National Corporation, Loret Group
  Other Country:
  Guadeloupe

- Southern Caribbean Fiber

  Owners:
  Digicel
  Other Countries:
  Antigua and Barbuda, Barbados, Dominica, Grenada, Guadeloupe, Martinique, Saint-Barthélemy, Saint Kitts and Nevis, Saint Lucia, Saint Martin, Saint Vincent and the Grenadines, Trinidad and Tobago

Landing 42 Tanguisson Point, Guam

Location: (-144.8°W, 13.55°N)

2 International Cables:

- Asia-America Gateway (AAG) Cable System

  Owners:
  Telekom Malaysia, AT&T, Starhub, PLDT, Communications Authority of Thailand, Airtel (Bharti), Telstra, Telkom Indonesia, BT, Eastern Telecom, PT Indonesia Satellite Corp., Spark New Zealand, Viettel Corporation, Saigon Postel Corporation, Vietnam Telecom International, Brunei International Gateway, BayanTel, Ezecom
  Other Countries:
  Brunei, China, Malaysia, Philippines, Singapore, Thailand, Vietnam

- Australia-Japan Cable (AJC)

  Owners:
  Softbank Telecom, Telstra, Verizon, AT&T
  Other Countries:
  Australia, Japan

Landing 43 Tuckerton, New Jersey, United States

Location: (74.34°W, 39.6°N)

2 International Cables:

- TAT-14

  Owners:
  BT, Verizon, Deutsche Telekom, Orange, Sprint, TeliaSonera, Level 3, KPN, Telenor, Etisalat, OTEGLOBE, SingTel, KDDI, Softbank Telecom, Zayo Group, Portugal Telecom, Slovak Telekom, TDC, Telus, Tata Communications, Telefonica, AT&T, Proximus, Elisa Corporation, Cyta, Rostelecom, Vodafone
  Other Countries:
  Denmark, France, Germany, Netherlands, United Kingdom

- GlobeNet

  Owners:
  BTG Pactual
  Other Countries:
  Bermuda, Brazil, Colombia, Venezuela

Landing 44 Tumon Bay, Guam

Location: (-144.8°W, 13.51°N)

2 International Cables:

- Guam Okinawa Kyushu Incheon (GOKI)

  Owners:
  AT&T
  Other Country:
  Japan

- Australia-Japan Cable (AJC)

  Owners:
  Softbank Telecom, Telstra, Verizon, AT&T
  Other Countries:
  Australia, Japan

Landing 45 Vero Beach, Florida, United States

Location: (80.39°W, 27.64°N)

1 International Cable:

- Bahamas 2

  Owners:
  AT&T, Telefonica, Verizon
  Other Country:
  Bahamas

Landing 46

Virginia Beach, Virginia, United States

Location: (76.06°W, 36.76°N)

3 International Cables:

- MAREA

  Owners:
  Facebook, Microsoft, Telxius
  Other Country:
  Spain

- Midgardsormen

  Owners:
  Midgardsormen
  Other Country:
  Denmark

- BRUSA

  Owners:
  Telxius
  Other Country:
  Brazil

Landing 47

Wall Township, New Jersey, United States

Location: (74.06°W, 40.15°N)

2 International Cables:

- Tata TGN-Atlantic

  Owners:
  Tata Communications
  Other Country:
  United Kingdom

- Seabras-1

  Owners:
  Seaborn Group
  Other Country:
  Brazil

International Submarine Cables Landing in the US

Cable 1 AEConnect (AEC)

More info:
http://www.aquacomms.com
Owners:
Aqua Comms
Length:
5,536 km
US Landing Point:

- Shirley, New York, United States

Other Country:
Ireland

Cable 2 America Movil Submarine Cable System-1 (AMX-1)

More info:
http://www.americamovil.com
Owners:
América Móvil
Length:
17,800 km
US Landing Points:

- Hollywood, Florida, United States
- Jacksonville, Florida, United States
- San Juan, Puerto Rico, United States

Other Countries:
Brazil, Colombia, Dominican Republic, Guatemala, Mexico

Cable 3 Americas-II

Owners:
Embratel, AT&T, Verizon, Sprint, CANTV, Tata Communications, Level 3, Telecom Argentina, Orange, Portugal Telecom, C&W Networks, Telecom Italia Sparkle, Entel Chile
Length:
8,373 km
US Landing Points:

- Hollywood, Florida, United States
- Miramar, Puerto Rico, United States
- St. Croix, Virgin Islands, United States

Other Countries:
Brazil, Curaçao, French Guiana, Martinique, Trinidad and Tobago, Venezuela

Cable 4 Antillas 1

Owners:
AT&T, Verizon, Sprint, Tata Communications, Orange, C&W Networks, Telecom Italia Sparkle, Embratel
Length:
650 km
US Landing Points:

- Isla Verde, Puerto Rico, United States
- Miramar, Puerto Rico, United States

Other Country:
Dominican Republic

Cable 5 Apollo

More info:
http://www.vodafone.com/business/article-cs-apollo-submarine-cable-system
Owners:
Vodafone
Length:
13,000 km
US Landing Points:

- Manasquan, New Jersey, United States
- Shirley, New York, United States

Other Countries:
France, United Kingdom

Cable 6 ARCOS

More info:
http://www.cwnetworks.com/
Owners:
C&W Networks, CANTV, Codetel, Hondutel, Belize Telemedia, Enitel, AT&T, Alestra, Verizon, RACSA, United Telecommunication Services (UTS), Telecarrier, Tricom USA, Telecomunicaciones Ultramarinas de Puerto Rico, Internexa, Orbinet Overseas, Telepuerto San Isidro, Bahamas Telecommunications Company, Instituto Costarricense de Electricidad, Orbitel
Length:
8,600 km
US Landing Points:

- North Miami Beach, Florida, United States
- Isla Verde, Puerto Rico, United States

Other Countries:
Bahamas, Belize, Colombia, Costa Rica, Curaçao, Dominican Republic, Guatemala, Honduras, Mexico, Nicaragua, Panama, Turks and Caicos Islands, Venezuela

Cable 7 Asia-America Gateway (AAG) Cable System

More info:
http://www.asia-america-gateway.com
Owners:
Telekom Malaysia, AT&T, Starhub, PLDT, Communications Authority of Thailand, Airtel (Bharti), Telstra, Telkom Indonesia, BT, Eastern Telecom, PT Indonesia Satellite Corp., Spark New Zealand, Viettel Corporation, Saigon Postel Corporation, Vietnam Telecom International, Brunei International Gateway, BayanTel, Ezecom
Length:
20,000 km
US Landing Points:

- Keawaula, Hawaii, United States
- San Luis Obispo, California, United States
- Tanguisson Point, Guam

Other Countries:
Brunei, China, Malaysia, Philippines, Singapore, Thailand, Vietnam

Cable 8 Atlantic Crossing-1 (AC-1)

More info:
http://www.level3.com
Owners:
Level 3
Length:
14,301 km
US Landing Point:

- Brookhaven, New York, United States

Other Countries:
Germany, Netherlands, United Kingdom

Cable 9 AURORA

More info:
http://fptelecoms.com/
Owners:
FP Telecommunications
Length:
n.a.
US Landing Point:

- Sarasota, Florida, United States

Other Countries:
Belize, Chile, Colombia, Costa Rica, Ecuador, Guatemala, Honduras, Mexico, Nicaragua, Panama

Cable 10 Australia-Japan Cable (AJC)

More info:
http://www.ajcable.com
Owners:
Softbank Telecom, Telstra, Verizon, AT&T
Length:
12,700 km
US Landing Points:

- Tanguisson Point, Guam
- Tumon Bay, Guam

Other Countries:
Australia, Japan

Cable 11 Bahamas 2

Owners:
AT&T, Telefonica, Verizon
Length:
470 km
US Landing Point:

- Vero Beach, Florida, United States

Other Country:
Bahamas

Cable 12 Bahamas Internet Cable System (BICS)

More info:
http://www.caribbeancrossings.com
Owners:
Caribbean Crossings
Length:
1,100 km
US Landing Points:

- Boca Raton, FL, United States
- Spanish River Park, Florida, United States

Other Country:
Bahamas

Cable 13 BRUSA

More info:
http://www.telxius.com
Owners:
Telxius
Length:
11,000 km
US Landing Points:

- San Juan, Puerto Rico, United States
- Virginia Beach, Virginia, United States

Other Country:
Brazil

Cable 14 Challenger Bermuda-1 (CB-1)

More info:
http://cableco.bm
Owners:
Cable Co.
Length:
1,448 km
US Landing Point:

- Charlestown, Rhode Island, United States

Other Country:
Bermuda

Cable 15 Colombia-Florida Subsea Fiber (CFX-1)

More info:
http://www.cwnetworks.com/
Owners:
C&W Networks
Length:
2,400 km
US Landing Point:

- Boca Raton, FL, United States

Other Countries:
Colombia, Jamaica

Cable 16 Columbus-III

Owners:
Telecom Italia Sparkle, AT&T, Verizon, Telefonica, Portugal Telecom, Tata Communications, Ukrtelecom, Telkom South Africa, Telecom Argentina, Instituto Costarricense de Electricidad, Embratel, Cyta
Length:
9,833 km
US Landing Point:

- Hollywood, Florida, United States

Other Countries:
Italy, Portugal, Spain

Cable 17 Crosslake Fibre

More info:
http://www.crosslakefibre.ca
Owners:
Crosslake Fibre
Length:
131 km
US Landing Point:

- Buffalo, New York, United States

Other Country:
Canada

Cable 18 Deep Blue Cable

More info:
http://www.deepbluecable.com
Owners:
Deep Blue Cable
Length:
12,000 km
US Landing Points:

- Boca Raton, FL, United States
- San Juan, Puerto Rico, United States
- Naples, FL, United States

Other Countries:
Anguilla, Aruba, Bonaire, Sint Eustatius, and Saba, Cayman Islands, Colombia, Curaçao, Dominican Republic, Haiti, Jamaica, Panama, Saint Martin, Trinidad and Tobago, Turks and Caicos Islands

Cable 19 FASTER

Owners:
Google, KDDI, SingTel, China Telecom, China Mobile, Global Transit
Length:
11,629 km
US Landing Point:

- Bandon, Oregon, United States

Other Countries:
Japan, Taiwan

Cable 20 FLAG Atlantic-1 (FA-1)

More info:
http://www.globalcloudxchange.com
Owners:
Global Cloud Xchange
Length:
14,500 km
US Landing Points:

- Island Park, New York, United States
- Northport, New York, United States

Other Countries:
France, United Kingdom

Cable 21 Gemini Bermuda

More info:
http://www.cwnetworks.com
Owners:
C&W Networks
Length:
1,287 km
US Landing Point:

- Manasquan, New Jersey, United States

Other Country:
Bermuda

Cable 22 Global Caribbean Network (GCN)

More info:
http://www.globalcaribbean.net
Owners:
Leucadia National Corporation, Loret Group
Length:
n.a.
US Landing Points:

- San Juan, Puerto Rico, United States
- St. Croix, Virgin Islands, United States

Other Country:
Guadeloupe

Cable 23 GlobeNet

More info:
http://www.globenet.net
Owners:
BTG Pactual
Length:
23,500 km
US Landing Points:

- Boca Raton, FL, United States
- Tuckerton, New Jersey, United States

Other Countries:
Bermuda, Brazil, Colombia, Venezuela

Cable 24 GTT Atlantic

More info:
http://www.gtt.net
Owners:
GTT
Length:
12,200 km
US Landing Point:

- Lynn, Massachusetts, United States

Other Countries:
Canada, Ireland, United Kingdom

Cable 25

Guam Okinawa Kyushu Incheon (GOKI)

More info:
http://www.att.com
Owners:
AT&T
Length:
4,244 km
US Landing Point:

- Tumon Bay, Guam

Other Country:
Japan

Cable 26

HANTRU1 Cable System

Owners:
Hannon Armstrong, Federated States of Micronesia Telecommunications Company, Marshall Islands Telecommunications Authority
Length:
2,917 km
US Landing Point:

- Piti, Guam

Other Country:
Federated States of Micronesia

Cable 27 Hawaiki

More info:
http://hawaikicable.co.nz
Owners:
Hawaiki Cable Company
Length:
14,000 km
US Landing Points:

- Kapolei, HI, United States
- Pacific City, OR, United States
- Pago Pago, American Samoa

Other Countries:
Australia, New Zealand

Cable 28 Hong Kong-Guam (HK-G)

Owners:
RTI Connectivity
Length:
3,900 km
US Landing Point:

- Piti, Guam

Other Country:
China

Cable 29 Honotua

More info:
http://www.opt.pf
Owners:
OPT French Polynesia
Length:
4,805 km
US Landing Point:

- Kawaihae, Hawaii, United States

Other Country:
French Polynesia

Cable 30 Japan-U.S. Cable Network (JUS)

Owners:
Verizon, AT&T, BT, Sprint, CenturyLink, KDDI, NTT, Chunghwa Telecom, Tata Communications, SingTel, Telekom Malaysia, Softbank Telecom, Orange, Level 3, SK Broadband, KT, China Telecom, China Unicom, LG Uplus, HKBN Enterprise Solutions, Starhub, PCCW, Telstra, Vodafone, PLDT
Length:
22,682 km
US Landing Points:

- Makaha, Hawaii, United States
- Manchester, California, United States
- Morro Bay, California, United States

Other Country:
Japan

Cable 31 JUPITER

Owners:
Amazon, Facebook, NTT, PLDT, PCCW, Softbank Telecom
Length:
14,000 km
US Landing Point:

- Hermosa Beach, California, United States

Other Countries:
Japan, Philippines

Cable 32 MAREA

Owners:
Facebook, Microsoft, Telxius
Length:
6,605 km
US Landing Point:

- Virginia Beach, Virginia, United States

Other Country:
Spain

Cable 33 Maya-1

More info:
http://www.maya-1.com
Owners:
Verizon, AT&T, Sprint, Hondutel, Telefonica, Orbitel, Telecom Italia Sparkle, C&W Networks, Entel Chile, Embratel, ETB, Axtel, Instituto Costarricense de Electricidad, Proximus, Prepa Networks, Orange, Tricom, RSL Telecom, América Móvil
Length:
4,400 km
US Landing Point:

- Hollywood, Florida, United States

Other Countries:
Cayman Islands, Colombia, Costa Rica, Honduras, Mexico, Panama

Cable 34 Midgardsormen

More info:
http://midgardsormen.net
Owners:
Midgardsormen
Length:
7,848 km
US Landing Point:

- Virginia Beach, Virginia, United States

Other Country:
Denmark

Cable 35 Monet

Owners:
Angola Cables, Google, Algar Telecom, Antel Uruguay
Length:
10,556 km
US Landing Point:

- Boca Raton, FL, United States

Other Country:
Brazil

Cable 36 New Cross Pacific (NCP) Cable System

Owners:
China Telecom, China Unicom, Chunghwa Telecom, KT, China Mobile, Microsoft, Softbank Telecom
Length:
13,618 km
US Landing Point:

- Pacific City, OR, United States

Other Countries:
China, Japan, Taiwan

Cable 37

Pacific Caribbean Cable System (PCCS)

Owners:
C&W Networks, Telconet, Setar, United Telecommunication Services (UTS), Telxius
Length:
6,000 km
US Landing Points:

- Jacksonville, Florida, United States
- San Juan, Puerto Rico, United States

Other Countries:
Aruba, Colombia, Curaçao, Ecuador, Panama

Cable 38

Pacific Crossing-1 (PC-1)

More info:
http://www.pc1.com
Owners:
NTT
Length:
20,900 km
US Landing Points:

- Grover Beach, California, United States
- Harbour Pointe, Washington, United States

Other Country:
Japan

Cable 39

Pacific Light Cable Network (PLCN)

More info:
http://pldc.com.hk
Owners:
Pacific Light Data Communication Co. Ltd., Google, Facebook
Length:
12,871 km
US Landing Point:

- El Segundo, California, United States

Other Countries:
China, Philippines, Taiwan

Cable 40

Pan-American Crossing (PAC)

More info:
http://www.level3.com
Owners:
Level 3
Length:
10,000 km
US Landing Point:

- Grover Beach, California, United States

Other Countries:
Costa Rica, Mexico, Panama

Cable 41 Pan American (PAN-AM)

Owners:
AT&T, Telefonica del Peru, Softbank Telecom, Telecom Italia Sparkle, Sprint, CANTV, Tata Communications, Telefónica de Argentina, Telstra, Verizon, Entel Chile, Telecom Argentina, Telconet, Instituto Costarricense de Electricidad, C&W Networks, Embratel
Length:
7,050 km
US Landing Point:

- St. Croix, Virgin Islands, United States

Other Countries:
Aruba, Chile, Colombia, Ecuador, Panama, Peru, Venezuela

Cable 42 PIPE Pacific Cable-1 (PPC-1)

More info:
http://www.pipenetworks.com/ppc1
Owners:
TPG
Length:
6,900 km
US Landing Point:

- Piti, Guam

Other Countries:
Australia, Papua New Guinea

Cable 43 Saint Maarten Puerto Rico Network One (SMPR-1)

Owners:
TelEm Group, Dauphin Telecom
Length:
375 km
US Landing Point:

- Isla Verde, Puerto Rico, United States

Other Countries:
Saint Martin, Sint Maarten

Cable 44 Samoa-American Samoa (SAS)

Owners:
American Samoa Government, Elandia
Length:
250 km
US Landing Point:

- Pago Pago, American Samoa

Other Country:
Samoa

Cable 45 Seabras-1

More info:
http://www.seabornnetworks.com
Owners:
Seaborn Group
Length:
10,800 km
US Landing Point:

- Wall Township, New Jersey, United States

Other Country:
Brazil

Cable 46 SEA-US

Owners:
RTI, Inc., Globe Telecom, Hawaiian Telcom, GTA TeleGuam, Telin, Balau Submarine Cable Company, Federated States of Micronesia Telecommunications Company
Length:
14,500 km
US Landing Points:

- Hermosa Beach, California, United States
- Makaha, Hawaii, United States
- Piti, Guam

Other Countries:
Federated States of Micronesia, Indonesia, Palau, Philippines

Cable 47 South America-1 (SAm-1)

More info:
http://www.telxius.com/
Owners:
Telxius
Length:
25,000 km
US Landing Points:

- Boca Raton, FL, United States
- San Juan, Puerto Rico, United States

Other Countries:
Argentina, Brazil, Chile, Colombia, Dominican Republic, Ecuador, Guatemala, Peru

Cable 48 South American Crossing (SAC)/Latin American Nautilus (LAN)

More info:
http://www.level3.com
Owners:
Level 3, Telecom Italia Sparkle
Length:
20,000 km
US Landing Point:

- St. Croix, Virgin Islands, United States

Other Countries:
Argentina, Brazil, Chile, Colombia, Panama, Peru, Venezuela

Cable 49 South America Pacific Link (SAPL)

More info:
http://www.oceannetworks.com
Owners:
Ocean Networks
Length:
17,600 km
US Landing Points:

- Jacksonville, Florida, United States
- Makaha, Hawaii, United States

Other Countries:
Chile, Panama

Cable 50 Southern Caribbean Fiber

More info:
http://www.southern-caribbean.com
Owners:
Digicel
Length:
n.a.
US Landing Points:

- San Juan, Puerto Rico, United States
- St. Croix, Virgin Islands, United States

Other Countries:
Antigua and Barbuda, Barbados, Dominica, Grenada, Guadeloupe, Martinique, Saint-Barthélemy, Saint Kitts and Nevis, Saint Lucia, Saint Martin, Saint Vincent and the Grenadines, Trinidad and Tobago

Cable 51 Southern Cross Cable Network (SCCN)

More info:
http://www.southerncrosscables.com
Owners:
Spark New Zealand, SingTel Optus, Verizon
Length:
30,500 km
US Landing Points:

- Hillsboro, Oregon, United States
- Kahe Point, Hawaii, United States
- Morro Bay, California, United States
- Spencer Beach, Hawaii, United States

Other Countries:
Australia, Fiji, New Zealand

Cable 52 TAT-14

More info:
https://www.tat-14.com
Owners:
BT, Verizon, Deutsche Telekom, Orange, Sprint, TeliaSonera, Level 3, KPN, Telenor, Etisalat, OTEGLOBE, SingTel, KDDI, Softbank Telecom, Zayo Group, Portugal Telecom, Slovak Telekom, TDC, Telus, Tata Communications, Telefonica, AT&T, Proximus, Elisa Corporation, Cyta, Rostelecom, Vodafone
Length:
15,295 km
US Landing Points:

- Manasquan, New Jersey, United States
- Tuckerton, New Jersey, United States

Other Countries:
Denmark, France, Germany, Netherlands, United Kingdom

Cable 53 Tata TGN-Atlantic

More info:
http://www.tatacommunications.com
Owners:
Tata Communications
Length:
13,000 km
US Landing Point:

- Wall Township, New Jersey, United States

Other Country:
United Kingdom

Cable 54 Tata TGN-Pacific

More info:
http://www.tatacommunications.com
Owners:
Tata Communications
Length:
22,300 km
US Landing Points:

- Hillsboro, Oregon, United States
- Los Angeles, California, United States
- Piti, Guam

Other Country:
Japan

Cable 55 Telstra Endeavour

More info:
https://www.telstraglobal.com
Owners:
Telstra
Length:
9,125 km
US Landing Point:

- Keawaula, Hawaii, United States

Other Country:
Australia

Cable 56 Trans-Pacific Express (TPE) Cable System

More info:
http://tpecable.org
Owners:
China Telecom, China Unicom, Chunghwa Telecom, KT, Verizon, NTT, AT&T
Length:
17,000 km
US Landing Point:

- Nedonna Beach, Oregon, United States

Other Countries:
China, Japan, Taiwan

Cable 57 Unity/EAC-Pacific

Owners:
Telstra, Google, Global Transit, SingTel, KDDI, Airtel (Bharti)
Length:
9,620 km
US Landing Point:

- Redondo Beach, California, United States

Other Country:
Japan

Cable 58 Yellow

More info:
http://www.level3.com
Owners:
Level 3
Length:
7,001 km
US Landing Point:

- Bellport, New York, United States

Other Country:
United Kingdom

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix K

This document was also filed as ECF No. 143-3 and can be found in this Joint Appendix at JA0286.

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix L

This document was also filed as ECF No. 168-28 and can be found in this Joint Appendix at JA3145.

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix M

This document was also filed as ECF No. 168-23 and can be found in this Joint Appendix at JA2743.

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix N

~~SECRET//ORCON,NOFORN~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

2011 AUG 16 PM 2:16

LEEANN FLYNN HALL

WASHINGTON, D.C.

[redacted]

NOTICE OF FILING OF GOVERNMENT'S SUPPLEMENT TO ITS SUBMISSIONS OF JUNE 1st AND JUNE 28TH, 2011

THE UNITED STATES OF AMERICA, through the undersigned Department of Justice attorney, respectfully submits the attached supplement in further support of the

~~SECRET//ORCON,NOFORN~~

Classified by: ~~Tashina Gauhar, Deputy Assistant Attorney General, NSD, DOJ~~
Reason: 1.4(c)
Declassify on: ~~16 August 2036~~

arguments set forth in submissions of June 1st and June 28th, 2011, concerning the above-referenced matters. This supplement explains the methodology behind and sets forth the results of a manual review by the National Security Agency (NSA) of a statistically representative sample of the nature and scope of the Internet communications acquired through NSA's FISA Amendments Act Section 702 upstream collection during a six-month period. The Government respectfully submits that the data provided herein supplements and supports the Government's Responses to the Court's Briefing Order of May 9th, 2011, and supplemental questions of June 17, 2011, and will further assist the Court in concluding that the certifications and procedures submitted in the above-referenced matters satisfy the requirements of the Act and are consistent with the Fourth Amendment to the Constitution of the United States. ~~(S//OC,NF)~~

Given the complex nature of the information provided in this supplement, the United States is prepared to provide any additional information the Court believes would aid it in reviewing these matters. The Government may also seek to supplement and/or clarify the information provided herein as appropriate during any hearing that the Court may hold in the above-captioned matters. ~~(S//OC,NF)~~

Respectfully submitted,

[redacted]

National Security Division
United States Department of Justice

(U//FOUO) NSA Characterization of Upstream Data: Process and Results

I. (U) Introduction

~~(TS//SI//NF)~~ This report explains the methodology behind and provides the results of a manual review of a statistically representative sample of Internet communications acquired through NSA's FISA Amendments Act (hereinafter "FAA") section 702 upstream collection during a six-month period.[1] The purpose of this review was to assemble data to assist the Court in understanding the nature and scope of the communications acquired through NSA's upstream collection. The data assembled consisted of:

- The volume of transactions containing single, discrete communications to, from, or about a selector used by a person targeted in accordance with NSA's section 702 targeting procedures (hereinafter "tasked selector") versus transactions containing multiple communications (hereinafter "Multi-communication Transactions" or "MCT") not all of which may be to, from, or about a tasked selector;[2]
- The types of discrete communications contained within MCTs [redacted]; and

[1] ~~(TS//SI//NF)~~ Additionally, as described on pages 8-9 of the Government's June 1, 2011 Response to the Court's Briefing Order of May 9, 2011, NSA conducted two tests of FAA 702 upstream collection in May 2011 using information from NSA's technical databases in an attempt to determine the likelihood of collecting an Internet transaction between a user in the United States and [redacted] NSA also attempted to further determine the extent to which those tests might be statistically representative of NSA's 702 upstream collection and repeated these tests in July 2011 using alternative data sets. Because of the technical limitations for automatically identifying transactions containing multiple communications, NSA assesses that the results of these tests are not comparable to each other or with the results of the separate manual analysis discussed herein. Furthermore, for the same reason of technical limitation, the results do not express as high a degree of granularity and accuracy as the manual analysis discussed herein, which took more than one month of careful review by experienced analysts to complete. None of the results discussed herein and in the Government's June 1 Response, however, are inconsistent.

[2] ~~(TS//SI//NF)~~ As described on pages 27-28 of the Government's June 1, 2011 Response to the Court's Briefing Order of May 9, 2011, NSA's inability to separate out individual pieces of information from Internet communications acquired by NSA's upstream collection systems does not extend to all forms of transactions. NSA has developed the capability to [redacted] identify transactions which [redacted] and, in certain other limited instances, transactions where an "active user" (as described more fully below) is a tasked selector. Based on a test of this capability from July 16th-29th 2011, NSA estimates that approximately only [redacted] of NSA's current upstream collection under FAA section 702 could be identified through [redacted] processes as communications to, from or about NSA's tasked selector. As reflected by the results of this manual review, this figure is significantly under-representative of the total proportion of NSA's upstream collection assessed to be communications to, from or about a tasked selector.

- The volume of MCTs that NSA assesses contain a wholly domestic communication not to, from, or about a tasked selector.[3]

II. (U) How the Statistically Representative Sample Was Assembled

~~(TS//SI//NF)~~ NSA assembled the sample of communications acquired through its upstream collection by first identifying all Internet communications acquired under section 702 – i.e., both from NSA upstream collection and collection from Internet service providers either by or with the assistance of the Federal Bureau of Investigation (hereinafter "PRISM collection") -- during a six-month period from January 1st through June 30th, 2011, and present within [redacted] as of July 14, 2011. As of that date, 140,974,921 Internet communications were present within [redacted] Of these, 127,718,854 (or approximately 91%) were acquired from PRISM collection, and 13,256,067 (or approximately 9%) were acquired through NSA's upstream collection.[6]

~~(TS//SI//NF)~~ The approximately 13.25 million Internet communications acquired through NSA's upstream collection (hereinafter "transactions") were then "shuffled" by NSA statisticians to ensure a random sample (i.e., any sample drawn would be statistically representative of the total 13.25 million transactions). NSA statisticians estimated that a manual review of a sample of approximately 50,000 of these randomized transactions would enable characterization of all 13.25 million transactions with a statistically high level of confidence and precision.[7]

III. (U) How the Manual Review Was Conducted and the Results of the Review

~~(TS//SI//NF)~~ Under the leadership of NSA's Deputy Director, an experienced interdisciplinary team consisting of experienced intelligence analysts, attorneys from NSA's Office of General Counsel, representatives from NSA's Office of the Director of Compliance, NSA statisticians, representatives from NSA's Network Analysis Center, and representatives from NSA's Office of Oversight and Compliance was assembled to conduct the review described herein and compile this report. A team of experienced NSA

---

[3] ~~(TS//SI//NF)~~ This aspect of the review required analysts to perform intensive analysis on discrete communications which did not contain the target's selector within MCTs, to determine if the sender and all intended recipients of those discrete communications were located in the United States. Such in-depth analysis is not typically conducted by analysts in their daily foreign intelligence analysis. Instead, an analyst would tend to focus his or her attention on those discrete communications within the MCT that are to, from, or about their assigned target, and would only perform a deeper inspection of those communications to confirm they were not wholly domestic if they were in-fact pertinent to the analyst's evaluation of foreign intelligence information and therefore worth further analysis for potential use.

[4] ~~(TS//SI//NF)~~ [redacted]

[5] ~~(TS//SI//NF)~~ This figure does not include Internet communications that were acquired during this six-month period but were purged prior to July 14, 2011.

[6] ~~(TS//SI//NF)~~ *See* Figure A of Appendix A, attached hereto.

[7] ~~(TS//SI//NF)~~ Details for the basis for NSA's statistical assertions are set forth in Appendix B, attached hereto.

intelligence analysts was assigned to conduct a manual review of the transactions. Ultimately, that team of NSA intelligence analysts collectively reviewed a total of 50,440 individual transactions.

~~(TS//SI//NF)~~ In order to ensure consistency among the analysts in their review, before beginning the manual review, the team members were trained to recognize MCTs and how to characterize the discrete communications contained within them. The team members were given training materials created specifically for this effort, which included screenshots depicting typical examples of the types of transactions acquired through NSA's upstream collection. NSA's Office of General Counsel, Office of Oversight and Compliance, and Office of the Director for Compliance reviewed all training materials and provided guidance throughout the manual review.

~~(TS//SI//NF)~~ For quality assurance, some transactions (approximately 10 out of every 5,000) underwent independent reviews by more than one analyst. In addition, the team lead performed spot reviews of transactions that had already undergone review (approximately 1 out of every 100). The team lead also personally reviewed any transaction that team members were unable to immediately characterize as clearly being a discrete communication or an MCT; as well as any MCT identified as potentially concerning a person located in the United States. Both the quality assurance overlap and the reviews performed by the team lead revealed no discrepancies among how analysts characterized any of the transactions subjected to these overlapping reviews.

~~(TS//SI//NF)~~ In conducting the manual review, NSA analysts took the following steps and made the following findings:

1. **Determined if the transaction was a single, discrete communication or an MCT.**[8] If the transaction was determined to be a single, discrete communication, no further analysis was done. Transactions determined to be MCTs were further analyzed, as described below.

   - Of the 50,440 transactions reviewed, 45,359 (approximately 90%) were determined to be single, discrete communications. The remaining 5,081 transactions (approximately 10%) were determined to be MCTs.[9]

2. **Characterized the discrete communications within the 5,081 MCTs as being** [redacted]

   - Of the 5,081 MCTs reviewed, [redacted]

[8] ~~(TS//SI//NF)~~ For any objects that the initial reviewer was uncertain about how to characterize (e.g., if the transaction contained data requiring further processing to render it intelligible to the analyst), the team lead performed a second review. As a result, each of 50,440 transactions reviewed were able to be characterized as being either a single, discrete communication or an MCT.

[9] ~~(TS//SI//NF)~~ *See* Figure B of Appendix A.

[10] ~~(TS//SI//NF)~~ [redacted]

[redacted][12]

3. **Determined whether the 5,081 MCTs contained any discrete communications as to which the sender and all intended recipients were located in the United States.** As discussed in more detail below, in many cases NSA analysts were able to make these determinations based on the location of the "active user" of the MCT.[13] In other cases, NSA had to rely on content analysis because the MCT did not contain technical information sufficient to identify the active user or to determine the active user's location. There were, however, instances where the MCT did not contain sufficient technical information or content for NSA to assess whether the MCT contained any wholly domestic communications.

   - Of the 5,081 MCTs, 713 (approximately 14%) had a tasked selector as the active user [redacted]. No further analysis of these MCTs was done to determine whether they contained wholly domestic communications. That is because the user of the tasked selector, who by operation of the NSA targeting procedures is a person reasonably believed to be located outside the United States, would be either the sender or an intended recipient of each of the discrete communications contained within the MCT.[14] Accordingly, all of the discrete communications within those MCTs would have at least one communicant reasonably believed to be located outside the United States (i.e., the target) and thus would not be wholly domestic.
   - Of the 5,081 MCTs, 2,668 (approximately 52%) had an active user that was not a tasked selector but was nonetheless an electronic communications account/address/identifier

[11] ~~(TS//SI//NF)~~ *See* Figure C of Appendix A.

[12] ~~(TS//SI//NF)~~ [redacted]

[13] ~~(TS//SI//NF)~~ When NSA acquires an Internet transaction between an individual using an electronic communications account/address/identifier and his/her service provider, that individual is the "active user" for that transaction. Such transactions can have, at most, one "active user."

[14] ~~(TS//SI//NF)~~ In this context, a communication to or from the target includes communications to or from the tasked selector itself (e.g., an e-mail sent to a tasked e-mail account), as well as communications where the tasked selector appears in other communications attributable to the target [redacted] *See In re DNI/AG Certificatio* [redacted] Docket No. 702(i)-08-01, Mem. Op. at 17 n.14 (USFISC Sept. 4, 2008).

reasonably believed to be used by a person located outside the United States.[15] No further analysis of these MCTs was done to determine whether they contained wholly domestic communications. That is because the foreign-based active user would be either a sender or intended recipient of each of the discrete communications within the transaction. Accordingly, all of the discrete communications within those MCTs would have at least one communicant reasonably believed to be located outside the United States (i.e., the foreign-based active user) and thus would not be wholly domestic.

- Of the 5,081 MCTs, 8 (approximately 0.16%) contained an electronic communication account/address/identifier of a non-targeted active user who appeared to be located in the United States, but none of the discrete communications within the MCT were determined to be wholly domestic because at least one of the communicants to each discrete communication was reasonably believed to be located outside the United States. Specifically, the 8 MCTs were determined to concern six non-targeted active users (i.e., two of the MCTs were duplicates):
  - Four MCTs (including both duplicates) [redacted] contained at least one e-mail message from a tasked selector as well as other e-mail messages from accounts/addresses/identifiers reasonably believed to be used by a person located outside the United States.[16] [redacted].
  - Three MCTs [redacted] with the users of accounts/addresses/identifiers who were reasonably believed to be located outside the United States.[17]
  - One MCT [redacted] where further technical analysis revealed that the active user was reasonably believed to be located outside the United States.
- Of the 5,081 MCTs, 10 (approximately 0.2%) contained an electronic communication account/address/identifier of a non-targeted active user who was located in the United States, and the MCTs contained at least one discrete communication that was wholly

[15] ~~(TS//SI//NF)~~ To determine the location of the non-targeted active user, NSA performed the same sort of [redacted] analysis it would perform before tasking an electronic communications account/address/identifier in accordance with its FAA Section 702 targeting procedures.

[16] ~~(TS//SI//NF)~~ To determine the location of the senders of each of these discrete e-mail messages, NSA performed the same sort of [redacted] analysis it would perform before tasking an electronic communications account/address/identifier in accordance with its FAA Section 702 targeting procedures.

[17] ~~(TS//SI//NF)~~ To determine the location of [redacted] NSA performed the same sort of [redacted] analysis it would perform before tasking an electronic communications account/address/identifier in accordance with its FAA Section 702 targeting procedures.

domestic. Specifically, all 10 of these MCTs were [redacted] and all 10 involved U.S.-based persons using [redacted].[18] For all 10 of these MCTs, only [redacted] was present. The [redacted] did not include [redacted].

- 9 of the 10 [redacted] were attributed to a single U.S.-based user. Each of these 9 [redacted] 10 total e-mail messages. The 9 [redacted] were not completely duplicative, but many of the 10 e-mail messages [redacted] were duplicative.
  - Two of the messages [redacted] in each of the 9 [redacted] contained a tasked selector and thus were not assessed to be wholly domestic.
  - Three of the messages [redacted] in each of the 9 [redacted] were [redacted] which is located in the United States) and thus were assessed to be wholly domestic.
  - The remaining e-mail messages [redacted] were between the U.S.-based user and persons reasonably believed to be located outside the United States (and thus not assessed to be wholly domestic) or whose location was unknown.[19]
- The other [redacted] was attributed to a different U.S.-based user. This [redacted] 15 total e-mail messages:
  - One of the [redacted] e-mail messages was from a tasked selector and thus was not assessed to be wholly domestic.
  - One of the [redacted] e-mail messages appeared to be a message that the U.S.-based user sent to himself [redacted] and thus was assessed to be wholly domestic.
  - One of the [redacted] e-mail messages appeared to be a message sent by an associate [redacted] account and thus was assessed to be wholly domestic.
  - The remaining e-mail messages [redacted] were between the U.S.-based user and persons reasonably believed to be

[18] ~~(TS//SI//NF)~~ [redacted]

[19] ~~(TS//SI//NF)~~ To determine the location of the other communicants, NSA performed the same sort of [redacted] analysis it would perform before tasking an electronic communications account/address/identifier in accordance with its FAA Section 702 targeting procedures.

located outside the United States and thus were not assessed to be wholly domestic.[20]

- Of the 5,081 MCTs, 1,682 (approximately 33%) required further, in-depth [redacted] analysis because they lacked information sufficient for NSA to readily identify the active user or determine the active user's location. In most of these cases, the transactions did not contain enough information for NSA to readily determine which electronic communication account/address/identifier appearing in the transaction was that of the active user. In other cases, NSA was able to determine which electronic communication account/address/identifier appearing in the transaction was that of the "active user," but NSA was unable to determine the active user's location. NSA's further [redacted] analysis of these 1,682 MCTs revealed:
  - For 1,220 of these 1,682 MCTs, NSA analysis of [redacted] data indicated that they were characteristic of a foreign use [redacted]
  - For 152 of these 1,682 MCTs, NSA analysis of [redacted] data indicated that they were [redacted]
  - For 86 of these 1,682 MCTs, NSA analysis of a combination of technical data and content revealed that they appeared to contain communications of persons located outside the United States (e.g., through further content analysis, NSA analysts were able to identify the active users of some MCTs and information indicative of those users' locations).
- Of the 5,081 MCTs, NSA cannot determine whether 224 MCTs contained wholly domestic communications, because these MCTs lack information sufficient for NSA to identify the active user or determine the active user's location. Nevertheless, NSA has no basis to believe any of these MCTs contain wholly domestic communications.
  - For 182 of these 224 MCTs, NSA technical analysis indicates that they were characteristic of [redacted]
  - For 1 of these 224 MCTs, NSA initially determined that it contained an electronic communication account/address/identifier of a non-targeted active user who appeared to be located in the United States, but whose location could not be determined upon further technical analysis. Specifically, [redacted]

[20] ~~(TS//SI//NF)~~ To determine the location of the other communicants, NSA performed the same sort of [redacted] analysis it would perform before tasking an electronic communications account/address/identifier in accordance with its FAA Section 702 targeting procedures.

[redacted]

- 23 of these 224 MCTs were not further analyzed because, although they were present in [redacted] as of the date the sample was assembled, they were subsequently purged and/or placed on NSA's Master Purge List.
- 18 of these 224 MCTs could not be further characterized by NSA analysts.

IV. (U) Conclusions Drawn from the Random Sample

~~(TS//SI//NF)~~ Based on a random sample of the approximately 13.25 million total Internet communications acquired by NSA through "upstream" techniques pursuant to FAA section 702 for the six-month period discussed, NSA assesses that the volume of transactions containing multiple communications not all of which may be to, from, or about a tasked selector is approximately between 1.29 and 1.39 million (9.70%-10.45%).[21] With respect to the types of discrete communications contained within multi-communication transactions manually reviewed by NSA analysts, [redacted]

~~(TS//SI//NF)~~ As described in Appendix B, which details NSA's Statistical Methodology for this review, the data compiled during the above-discussed manual review of a random sample of Internet communications acquired during a six-month period can be used to characterize with a statistically high degree of confidence (i.e., a simultaneous confidence level of 95% for these intervals collectively) the nature and scope of the entirety of the approximately 13.25 million Internet communications from

[21] ~~(TS//SI//NF)~~ As calculated in the attached Appendix detailing NSA's Statistical Methodology for this review, these figures are based on the 45,359 of the 50,440 transactions (89.93%) manually reviewed by NSA analysts as containing single, discrete communications and the 5,081 transactions (10.07%) manually reviewed by NSA analysts as containing multiple communications. *See also* Step 1, *supra* page 3.

[22] ~~(TS//SI//NF)~~ [redacted]

[23] ~~(TS//SI//NF)~~ [redacted]

[24] ~~(TS//SI//NF)~~ [redacted]

which the random sample was drawn. Specifically, NSA assesses that of these approximately 13.25 million Internet communications acquired through NSA upstream collection:

- between approximately 11.87 and 11.97 million (89.55%-90.30%) are transactions that contain only single, discrete communications to, from, or about a tasked selector;
- between 168,853 and 206,922 (1.27%-1.56%)[25] are transactions that contain multiple communications, all of which are either to or from a tasked selector;
- between 1,042,838 and 1,113,947 (7.87%-8.53%)[26] are transactions that contain multiple communications, at least one of which is to, from, or about NSA's tasked selector, but all of which are believed to either be to or from non-targeted persons reasonably believed to be located outside the United States;
- between 48,609 and 70,168 (0.37%-0.53%)[27] are transactions that contain multiple communications, at least one of which is to, from, or about NSA's tasked selector, and at least one of which is a communication between non-targeted persons (i.e., not to, from or about a tasked selector) that lacks sufficient information for NSA to identify the location of the sender and all intended recipients of that communication; and
- between 996 and 4,965 (0.0075%-0.0375%) contain a wholly domestic communication not to, from, or about a tasked selector.

~~(TS//SI//NF)~~ In sum, while there was insufficient information present for 224 multi-communication transactions for NSA analysts to characterize the likelihood that they may contain wholly domestic communications (the majority of which were attributable to [redacted], for the reasons explained in detail

---

[25] ~~(TS//SI//NF)~~ As calculated in the attached Appendix, these figures are based on 713 of the 5,081 MCTs (14.03%) and 50,440 total transactions (1.41%) reviewed by NSA analysts as containing a tasked selector as the active user [redacted]. See also Step 3, *supra* page 4.

[26] ~~(TS//SI//NF)~~ As calculated in the attached Appendix, these figures are based on 4,134 of the 5,081 MCTs (81.36%) and 50,440 total transactions (8.19%) reviewed by NSA analysts as containing discrete communications believed to be to or from non-targeted persons located outside the United States. More specifically, this total includes the following MCTs manually reviewed by NSA analysts: 2,668 that had an active user reasonably believed to be a person located outside the United States; 8 that included at least one communicant reasonably believed to be located outside the United States for each communication therein; 1,220 that are characteristic o[redacted] 152 that are indicative of [redacted] and 86 that all communications contained therein were to or from persons located outside the United States. *See* Step 3, *supra* pages 4-6.

[27] ~~(TS//SI//NF)~~ As calculated in the attached Appendix, these figures are based on 224 of the 5,081 MCTs (4.41%) and 50,440 total transactions (0.44%%) reviewed by NSA analysts that lacked sufficient information to identify the active user or the active user's location. *See* Step 3, *supra* page 6.

above, NSA has no basis to believe any of the remaining Internet communications reviewed in the 50,440 sample are wholly domestic beyond those 10 discussed above.[28] Moreover, each of those 10 Internet communications has been placed on NSA's Master Purge List.

----- *The remainder of this page intentionally left blank.* -----

[28] ~~(TS//SI//NF)~~ *See* Figure D of Appendix A.

~~TOP SECRET//COMINT//NOFORN~~

(U) VERIFICATION

(U) I declare under penalty of perjury that the facts set forth in the foregoing "NSA Characterization of Upstream Data: Process and Results" are true and correct based upon my best information, knowledge and belief. Executed pursuant to Title 28, United States Code, § 1746, on this 16th day of August, 2011.

[redacted]

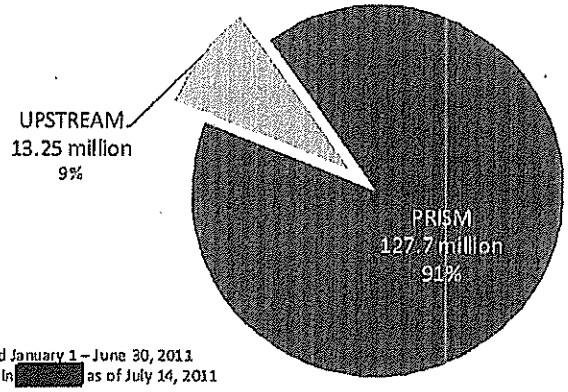
Signals Intelligence Directorate Compliance Architect
National Security Agency

~~TOP SECRET//COMINT//NOFORN~~

Appendix A

Fig. A Total FAA 702

140,974,921 Internet Communications



Acquired January 1 – June 30, 2011
Present in [redacted] as of July 14, 2011

Fig. B Total Upstream Sample

50,440 objects manually reviewed

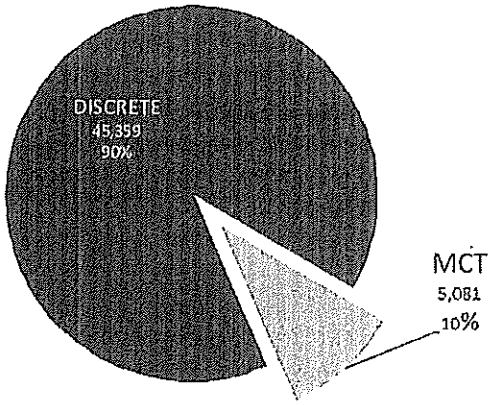


Fig. C MCT Type

5,081 objects

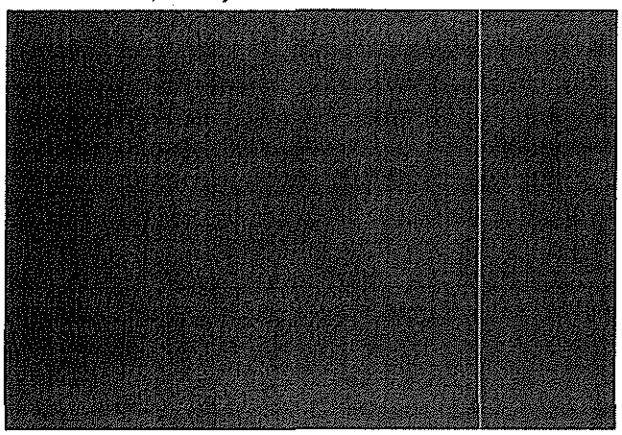
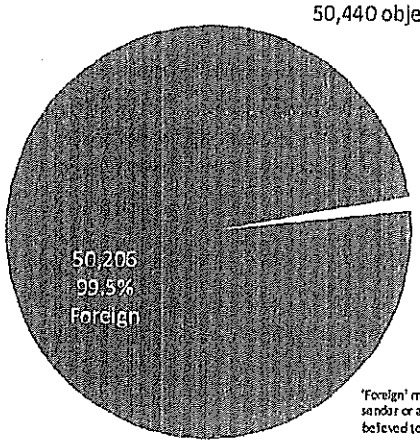


Fig. D Summary

50,440 objects



'Foreign' means a transaction in which at least the sender or an intended recipient is reasonably believed to be located outside the United States.

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20360801

~~TOP SECRET//COMINT//NOFORN~~

Appendix B: Statistical Methodology – FAA Section 702 Upstream Manual Review

~~(TS//SI//NF)~~ Using statistical analysis NSA determined the proportions of transactions satisfying certain criteria (e.g., proportion of FAA Section 702 upstream Internet transactions that are Multi-communication Transactions (MCT) versus transactions containing single, discrete communications). As further described below, transactions were categorized in various ways. The categorization process can be complex; to minimize categorization error, NSA used a statistical approach involving actual examination of an appropriate sample of transactions by experienced intelligence analysts. (The use of only a sample is a concession to the large volume of transactions and the labor-intensive nature of the categorization process.) That is, NSA traded "categorization error" for "statistical error"; the latter refers to the fact that by considering only a randomly sampled portion of the universe of transactions, NSA estimated the true proportions (as they exist in the universe) -- with error bounds and levels of confidence that can be stated justifiably.

~~(TS//SI//NF)~~ **THE SAMPLE.** As discussed more fully in the "NSA Characterization of Upstream Data: Process and Results," NSA identified 13,256,067 transactions acquired through NSA's FAA 702 upstream collection during a six-month period from January 1st through June 30th, 2011. Of those approximately 13.25 million transactions, a team of experienced intelligence analysts carefully examined 50,440 over a nearly one-month time period. The transactions were presented to the analysts in a randomized order, ensuring that a simple random sample would serve as the basis for conclusions -- supported by statistical theory – about the true proportions of the 13.25 million-transaction universe.

~~(TS//SI//NF)~~ **ESTIMATES AND CONFIDENCE INTERVALS.** The proportions formed from the sampled transactions serve as unbiased estimates of the corresponding proportions of the 13,256,067-transaction universe. Further, for (six) selected proportions, NSA states a confidence interval for each. Collectively, these intervals have a simultaneous confidence level of 95%. This means that the intervals were produced by a procedure calibrated to produce, for at least 95% of the sample sets NSA could have drawn, intervals which all cover the corresponding true (i.e., universal) proportions. Individually, each interval has a higher level of confidence associated with it; component confidence levels are quoted below.

~~(TS//SI//NF)~~ For each of the six categories, NSA also states a confidence interval for the actual number of that category's transactions within the 13,256,067-transaction (January-June, 2011 upstream) universe. Such an interval is simply an equivalent representation of the corresponding proportion-interval (it is obtained by multiplying the endpoints of the proportion-interval by 13,256,067), and so the inclusion of such intervals does not affect the (95%) level of simultaneous confidence.

~~(TS//SI//NF)~~ Specifically: By sampling a subset of the universe (or *population*) of upstream transactions, NSA estimated the following six proportions. (Hereinafter, N denotes 13,256,067 – the size of that universe; M denotes the (unknown) actual number of MCTs in that universe).

- M / N: the proportion of the population comprising MCTs;

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20360801

- 1-(M/N): the proportion of the population comprising discrete transactions;
- the proportion of the population comprising MCTs in which all communications are either to or from NSA's tasked selector (hereinafter labeled "Target" MCTs);
- the proportion of the population comprising MCTs in which all communications are believed to either be to or from non-targeted persons located outside the United States (hereinafter labeled "Foreign" MCTs);
- the proportion of the population comprising MCTs in which the nature of one or more communications between non-targeted persons lacked sufficient information for NSA analysts to identify the location of the sender and all intended recipients (hereinafter labeled "Unknownable" MCTs);
- the proportion of the population comprising MCTs that NSA analysts assessed contain a wholly domestic not to, from, or about a tasked selector (hereinafter labeled "Confirmed Wholly Domestic").

~~(TS//SI//NF)~~ (The first of these proportions equals the total of the last four.) In the following, lower-case letters denote transaction counts as realized in the sample, in categories corresponding to their upper-case counterparts. That is, n is the number of transactions sampled (this turned out to be 50,440), and m is the number of MCTs in the sample.

~~(TS//SI//NF)~~ **OUTLINE OF PROCEDURE.** NSA designed a procedure that accepts a size-n *simple random sample*[1] of the population, and produced from it estimates and confidence intervals for the six "true"[2] proportions NSA sought. The estimates NSA produced are simply the corresponding proportions as found in the sample – e.g., the sample proportion m/n was NSA's estimate of the population proportion M/N; such a sample proportion is unbiased[3] for its population counterpart, meaning that were a sample proportion to be computed for each of the possible size-n samples that could be drawn, the average of these sample proportions would equal the "true" (population) proportion.

---

[1] ~~(TS//SI//NF)~~ A simple random sample is one that is drawn in a way that ensures that all possible size-n subsets of the (size-N) population have an equal chance of being selected; this sampling technique enables statistically justifiable claims by avoiding potential (known or unknown) sources of bias in the population (e.g., a periodic trend in the population over time).

[2] ~~(TS//SI//NF)~~ "True" refers to proportions that relate to the entire population, which cannot be determined for certain, as n is smaller than N.

[3] ~~(TS//SI//NF)~~ Unbiasedness means that the estimate is aiming for the right "target"; however, it indicates nothing about the precision of the estimate. An estimation procedure can be unbiased whether it is based on a small or large sample size n.

~~(TS//SI//NF)~~ To express precision appropriately, NSA designed its procedure to produce confidence intervals – one for each of the (six) population proportions of interest – having a simultaneous confidence level of 95%. This means that:

- Based on a sample, the procedure will produce a collection of intervals, each asserted to contain the true (population) proportion it targets.

- Because the procedure operates on a random sample, the interval endpoints are *random variables*; the particular collection of intervals a particular sample yields may fail to cover one or more of the population proportions it targets. But the procedure is designed so that this failure probability – *whatever* the true proportions are – is no more than 5%; that is, for at least 95% of the (size-n) simple random samples it might process, the procedure will produce intervals which *all* cover their targeted population proportions.

- In order to achieve this level of confidence about a collection of intervals simultaneously, the procedure is designed so that the respective failure probabilities associated with the component intervals total no more than 5%. In particular, this 5% was allocated as follows:

  - 2.5% to the proportion of "Confirmed Wholly Domestic";
  - 0.67% to each of the "Target," "Foreign," "Unknown" proportions;
  - 0.5% to the proportion of MCT (i.e., M/N). As the proportions of discrete and MCT transactions are complementary (i.e., they total 1), the confidence interval for the proportion of discrete transactions is obtained by subtracting each of the endpoints for the MCT-interval from 1 – and it is the case that one of these intervals will cover its population target if and only if the other does. Therefore, there is no need to separately allocate "failure probability" to the proportion-of-discrete.

~~(TS//SI//NF)~~ The probability of drawing a sample resulting in one or more "failing" intervals is no more than the sum of the failure probabilities of the respective component intervals, hence the claim of 95% confidence for the procedure outlined here. The "no more" qualification makes this technique conservative: relationships (complicated and left unanalyzed) between the random variables involved may make the practical confidence level higher; 95% represents a worst-case claim. To achieve simultaneous 95% confidence, the 5% failure probability could have been allocated in any way. (Broadly: the lower the confidence level (i.e., the higher the failure probability), the narrower the intervals the procedure will produce. An extreme example: a procedure for 100% confidence intervals would produce uselessly wide intervals, as it would have to be able to claim that its intervals cover truth for *every* possible size-n sample it could have received.) This procedure for simultaneous intervals is conservative in a further way: Just as the sum of the discrete and MCT proportions equals 1, so does the sum of the discrete, "Target," "Foreign," "Unknown," and "Confirmed Wholly Domestic" proportions. It is difficult to exploit this latter constraint properly; NSA utilized the conservative method described here to ensure that its assertions about the procedure's performance are valid.

~~(TS//SI//NF)~~ **CONFIDENCE-INTERVAL PROCEDURE FOR A SINGLE PROPORTION.** As outlined above, the procedure for (95%) simultaneous confidence intervals was achieved by producing component confidence intervals based on (individually higher) levels of confidence (e.g., 99.5% for M/N). The construction of component confidence intervals can be understood via the following example, using the M/N target. For the sample of size n to be observed, m represents the (random) number of MCTs to be realized in the sample. Formally, m has a *hypergeometric* distribution (arising from sampling transactions "without replacement"); to make the mathematical computations tractable, NSA approximated this distribution by a *binomial* distribution corresponding to sampling *with* replacement (in which each sampled transaction would be replaced after it is drawn, and hence would be eligible to be drawn multiple times). This approximation is uniformly conservative; i.e., it will result in wider intervals. The proportion to be estimated, M/N, appears as the (unknown) parameter (now denoted p) of this binomial distribution. Treating m as a binomial random variable based on n *trials*, NSA used an accepted method (the *Clopper-Pearson* method) as the basis to devise its confidence-interval procedure for p. (Below, the notation $B(n,q)$ refers to an n-trial binomial random variable having parameter q.) Upon observing m, NSA:

- Determines, for each of various proportions x between 0 and 0.5%, parameters q and r such that
  - x is the probability that a $B(n,q)$ random variable takes a value of at least m (but if m=0, take q to be 0);
  - (0.5% - x) is the probability that a $B(n,r)$ random variable takes a value no larger than m (but if m=n, take r to be 1).

  r exceeds q; the pair $[q,r]$ determines an interval.

- Determines the narrowest of all such intervals $[q,r]$ and reports it as the (99.5%) confidence interval for $p = M/N$.

~~(TS//SI//NF)~~ Practically, the q's and r's can be computed using *inverse Beta functions*, and computer software can find the narrowest interval efficiently.

Remainder of this page intentionally left blank.

RESULTS:

	# of transactions in sample	Sample proportion (of 702 upstream)	Confidence interval for corresponding universal proportion	Confidence interval for the actual number (of the 13.25 million)
Discrete	45,359	0.8993	0.8955 – 0.9030	11,870,284 – 11,970,275
MCT	5,081	0.1007	0.0970 – 0.1045	1,285,792 – 1,385,783

	# of transactions in sample	Sample proportion (of MCT)	Confidence interval for corresponding universal (MCT) proportion	Confidence interval for the actual number (of the 13.25 million)
TARGET	713	0.01414	0.01274 – 0.01561	168,853 – 206,922
FOREIGN	4,134	0.08196	0.07867 – 0.08532	1,042,838 – 1,130,947
UNKNOWABLE	224	0.004441	0.003667 – 0.005293	48,609 – 70,168
CONFIRMED WHOLLY DOMESTIC	10	0.0001983	0.00007508 – 0.0003746	996 – 4,965

[redacted]

Remainder of this page intentionally left blank.

VERIFICATION

I declare under penalty of perjury that the facts set forth in this Appendix are true and correct based upon my best information, knowledge and belief. Executed pursuant to Title 28, United States Code, Section 1746, on this 11th day of August, 2011.

[redacted]
[Statistician]
National Security Agency

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix O

~~TOP SECRET//COMINT//ORCON/NOFORN~~

JOINT STATEMENT OF

LISA O. MONACO
ASSISTANT ATTORNEY GENERAL
FOR NATIONAL SECURITY
U.S. DEPARTMENT OF JUSTICE

JOHN C. (CHRIS) INGLIS
DEPUTY DIRECTOR
NATIONAL SECURITY AGENCY

ROBERT S. LITT
GENERAL COUNSEL
OFFICE OF DIRECTOR OF NATIONAL INTELLIGENCE

BEFORE THE
PERMANENT SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES HOUSE OF REPRESENTATIVES

AT A HEARING CONCERNING
"FISA AMENDMENTS ACT REAUTHORIZATION"

PRESENTED ON
DECEMBER 8, 2011

[redacted]

Joint Statement of

Lisa O. Monaco
Assistant Attorney General
for National Security
U.S. Department of Justice

John C. (Chris) Inglis
Deputy Director
National Security Agency

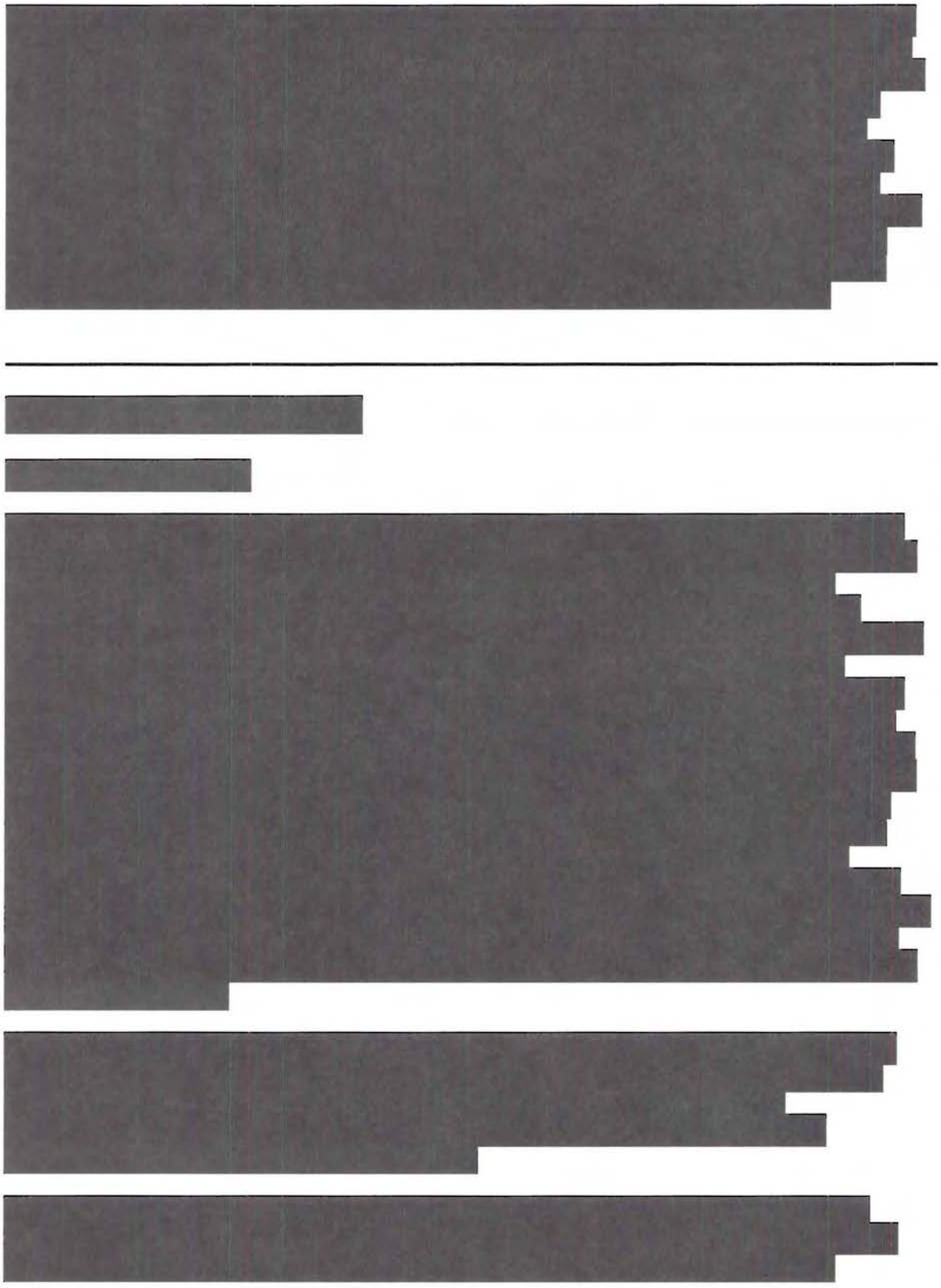
Robert S. Litt
General Counsel
Office of Director of National Intelligence

Before the
Permanent Select Committee on Intelligence
United States House of Representatives

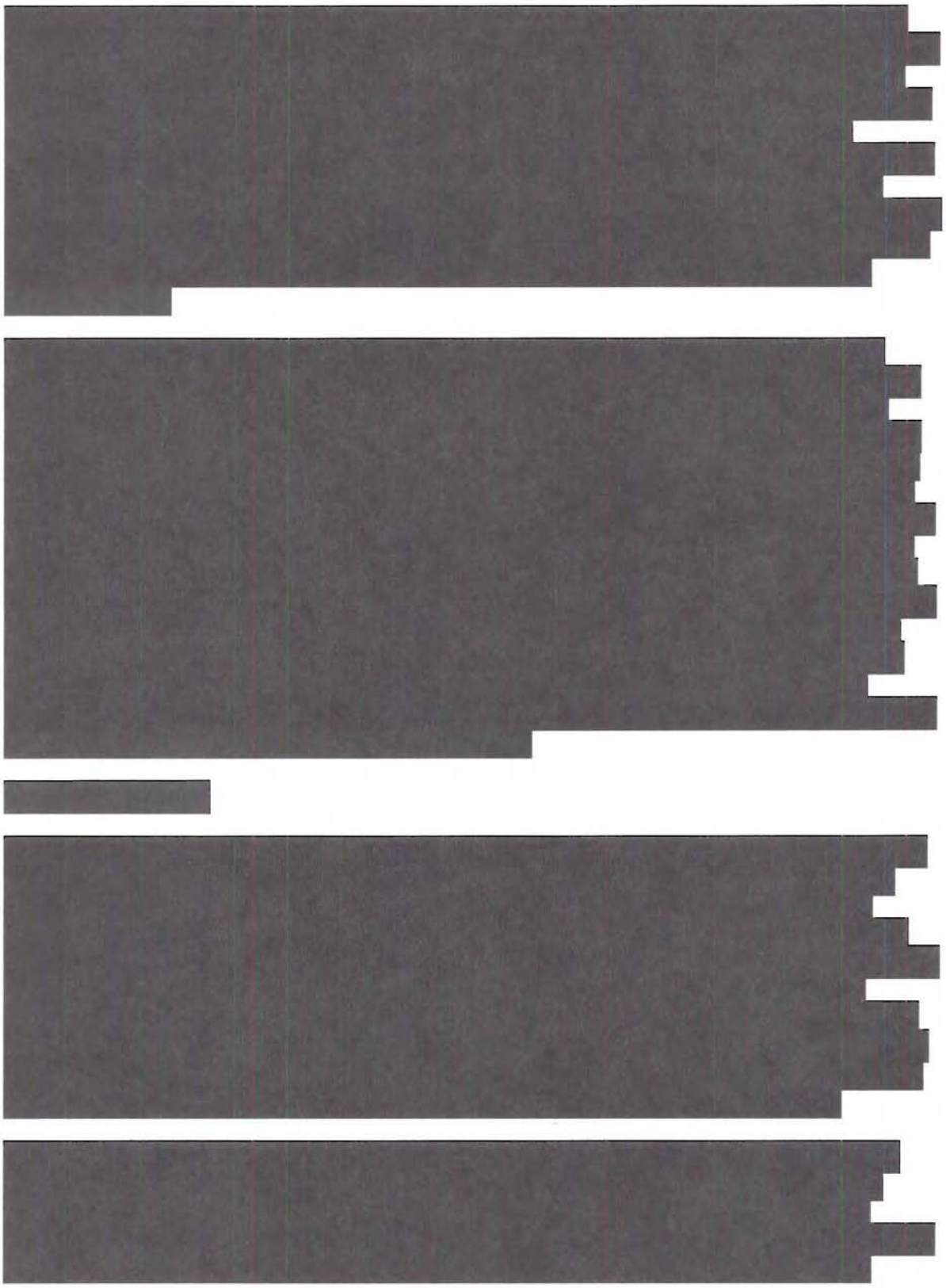
At a Hearing Concerning
"FISA Amendments Act Reauthorization"

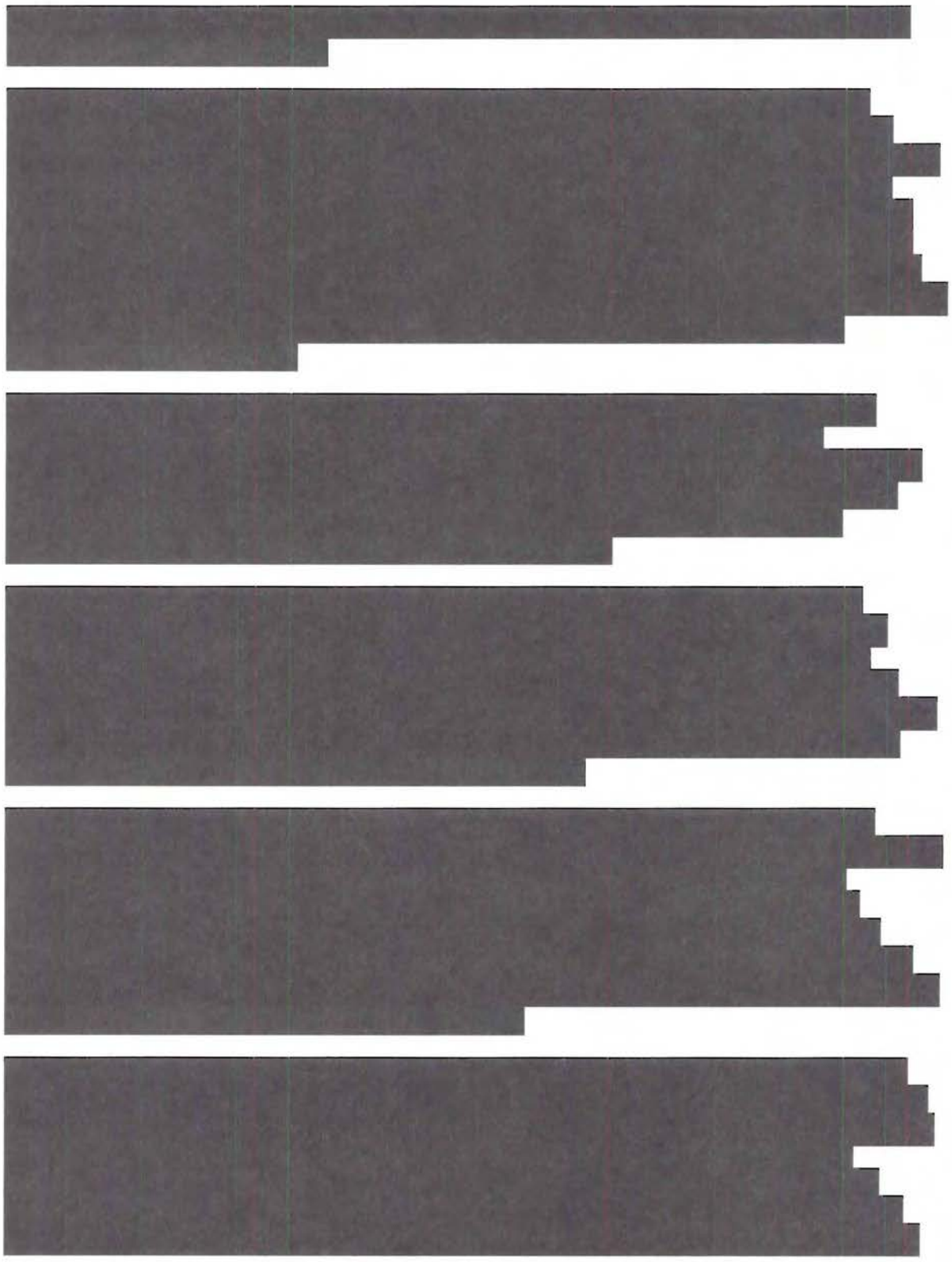
Presented on
December 8, 2011

[redacted]

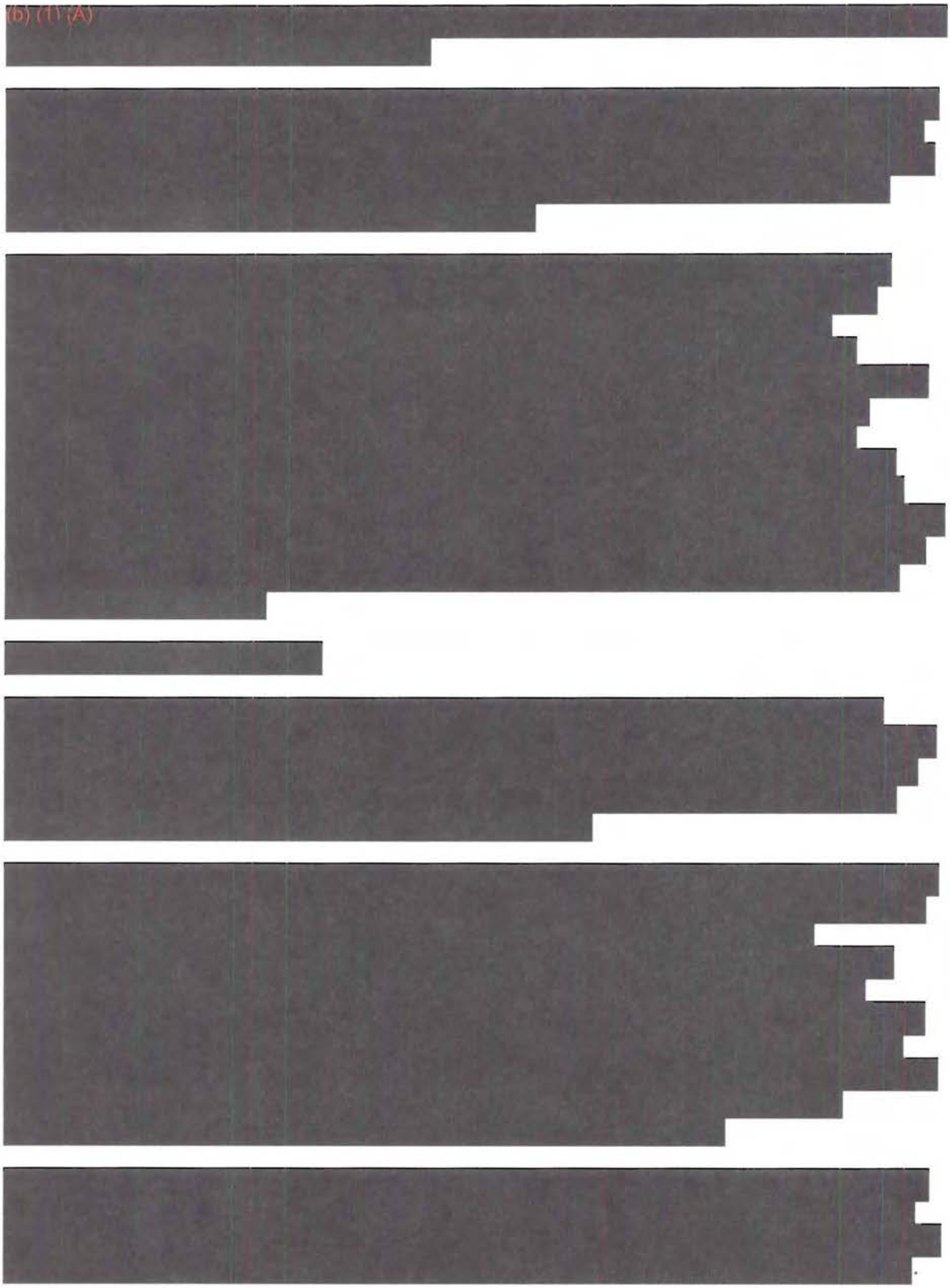


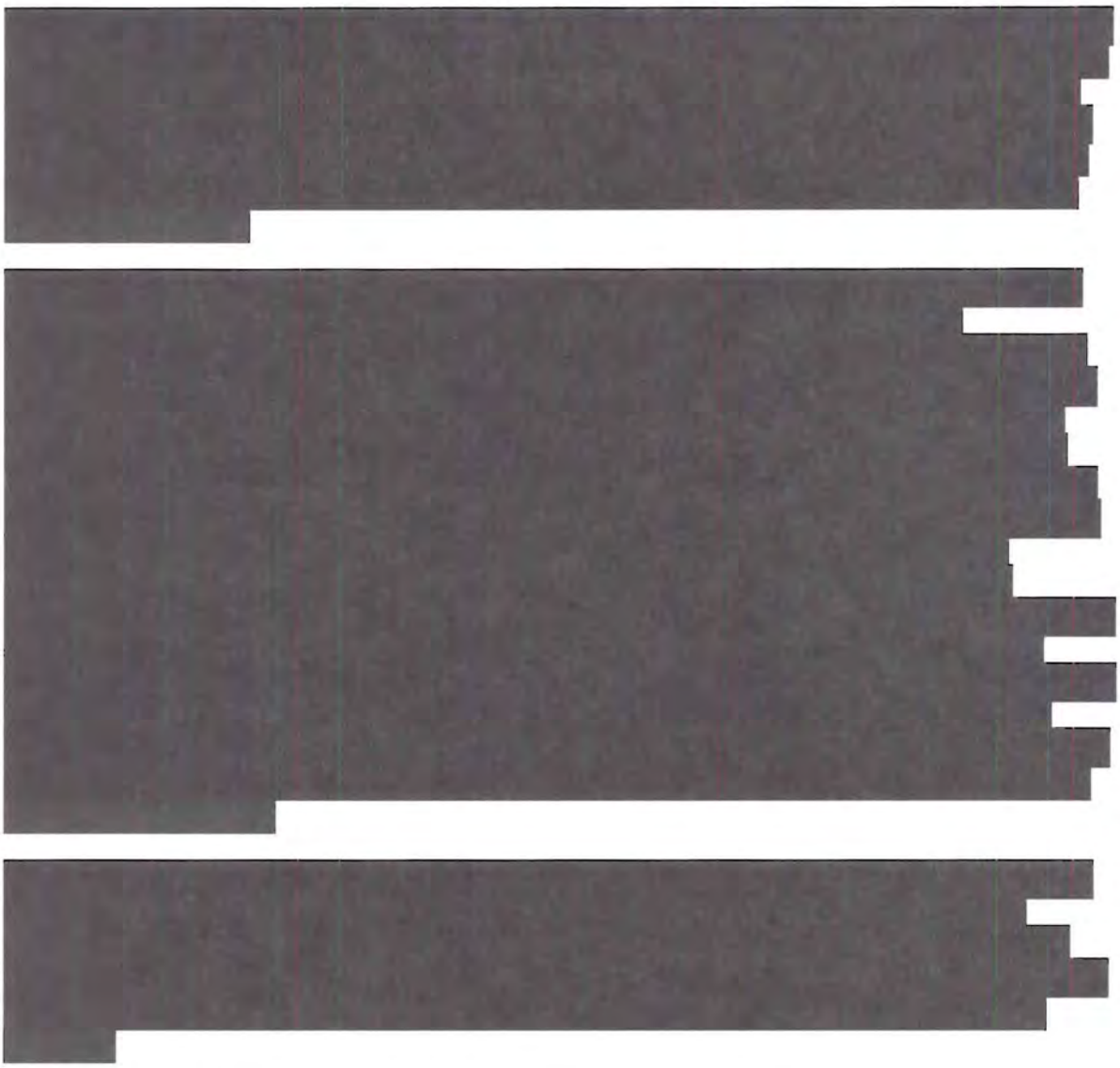
~~TOP SECRET//COMINT//ORCON/NOFORN~~





(b) (1) (A)





(U) **Recent FISC Opinion**

~~(TS//SI//NF)~~ On October 3, 2011, the FISC issued an opinion addressing the Government's submission of replacement certifications under section 702. *In re DNI/AG Certification 2009-C, et. al.,* , Mem. Op. The FISC approved most of the Government's submission. It upheld NSA's and FBI's targeting procedures, CIA's and FBI's minimization procedures, and most of NSA's minimization procedures. Nevertheless, the FISC denied in part the Government's requests because of its concerns about the rules governing the retention of certain non-targeted Internet communications acquired through NSA's upstream collection. The FISC's exhaustive analysis of the Government's submission, like its other decisions, refutes any argument that the court is a "rubber stamp," and demonstrates the rigorous nature of the oversight it conducts.

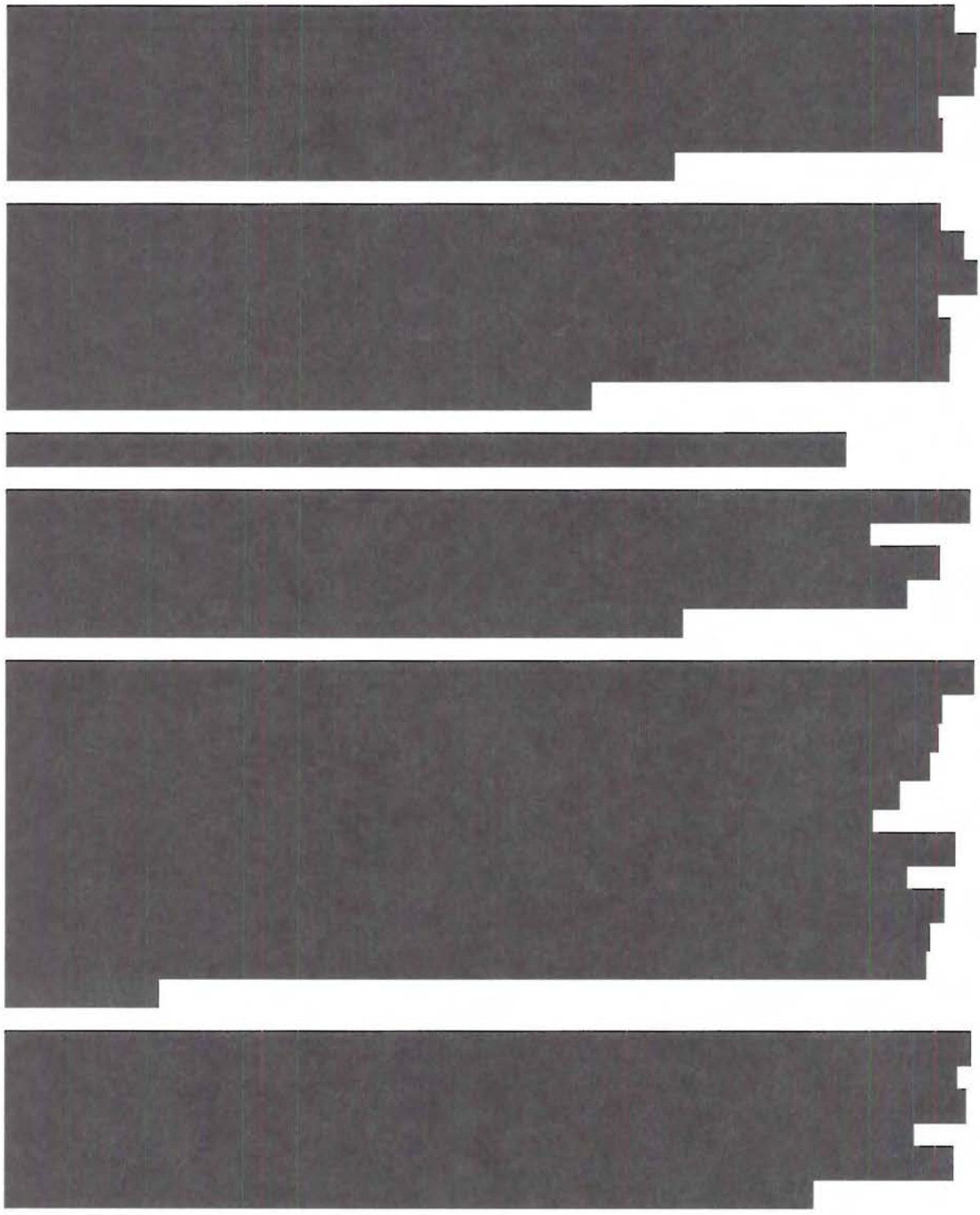
~~(TS//SI//NF)~~ As described above, upstream collection allows NSA to acquire, among other things, communications about a target where the target is not itself a communicant. In doing so, NSA uses [redacted] that are reasonably designed to screen out communications that are wholly domestic in nature, in accordance with section 702's requirements. Although reasonably designed to accomplish this result, [redacted] are not perfect. In addition, upstream collection devices acquire Internet "transactions" that include tasked selectors. Such a transaction may consist of a single communication (a "single-communication transaction," or SCT) or multiple communications sent in a single transaction (a "multi-communication transaction," or MCT) [redacted] In such instances, upstream collection acquires the entire MCT, which in all cases will include a communication to, from, or about a tasked selector but in some cases may also include communications that are not about a tasked selector and may have no relationship, or no more than an incidental relationship, to the targeted selector. Thus although upstream collection only targets Internet communications that are not between individuals located in the United States and are to, from, or about a tasked account, there is some inevitable incidental collection of wholly domestic communications or communications not to, from, or about a tasked account that could contain U.S. person information. Based on a sample reviewed by NSA, the percentage of such communications is very small (about .02%), but given the volume of the upstream collection, the FISC concluded that the actual number of such communications may be in the tens of thousands annually.

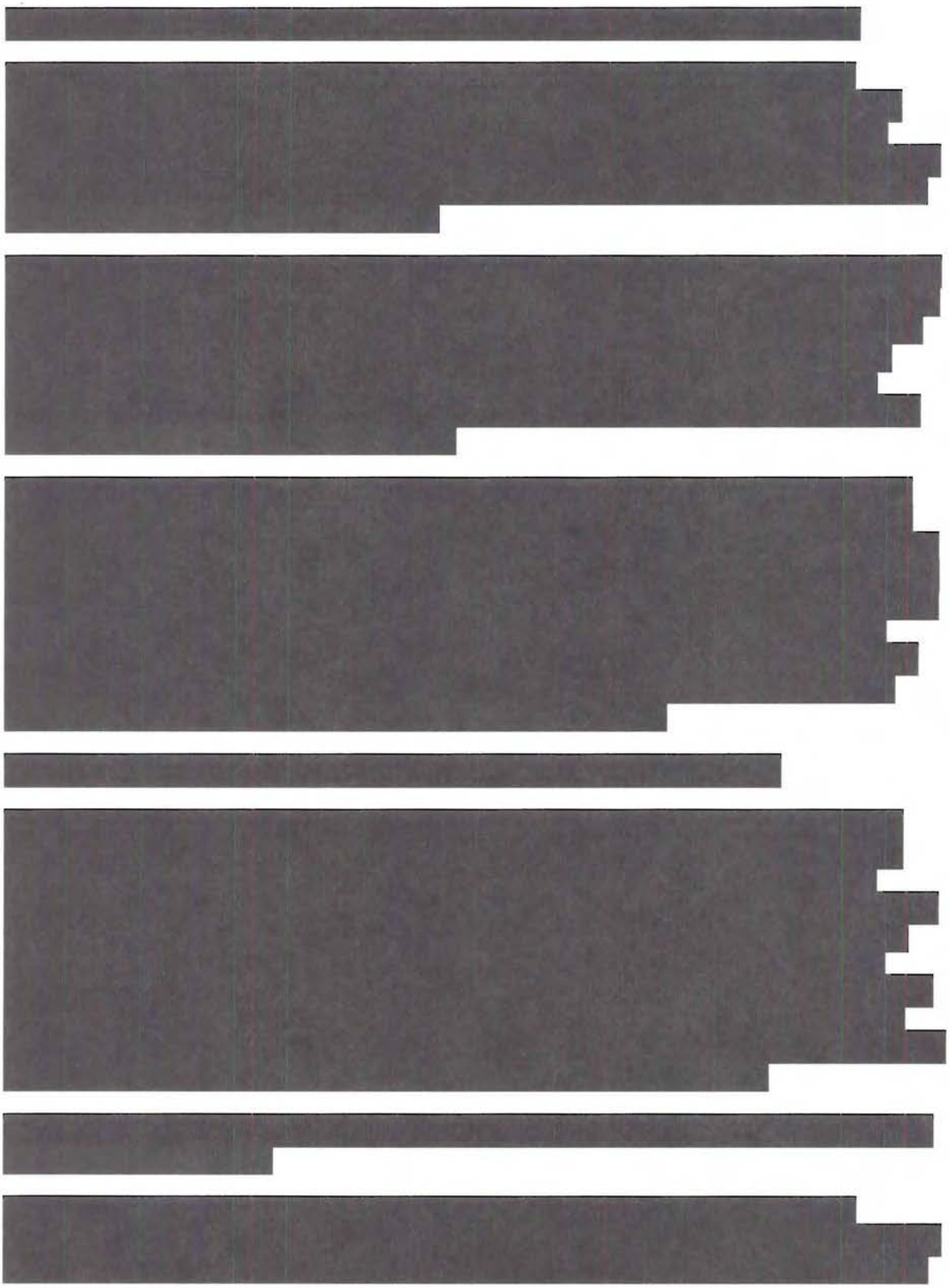
~~(TS//SI//NF)~~ The FISC upheld NSA's continued upstream acquisition of Internet communications under section 702 even though it includes the unintentional acquisition of wholly domestic communications and the incidental acquisition of MCTs that may contain one or more individual communications that are not to, from, or about the tasked selector. *See id.* at 74, 78-79. The FISC also reaffirmed that the acquisition of foreign intelligence information under section 702 falls within the foreign intelligence exception to the warrant requirement of the Fourth Amendment, and confirmed that nothing had disturbed its "prior conclusion that the government is not required to obtain a warrant before conducting acquisitions under NSA's targeting and minimization procedures." *Id.* at 69.

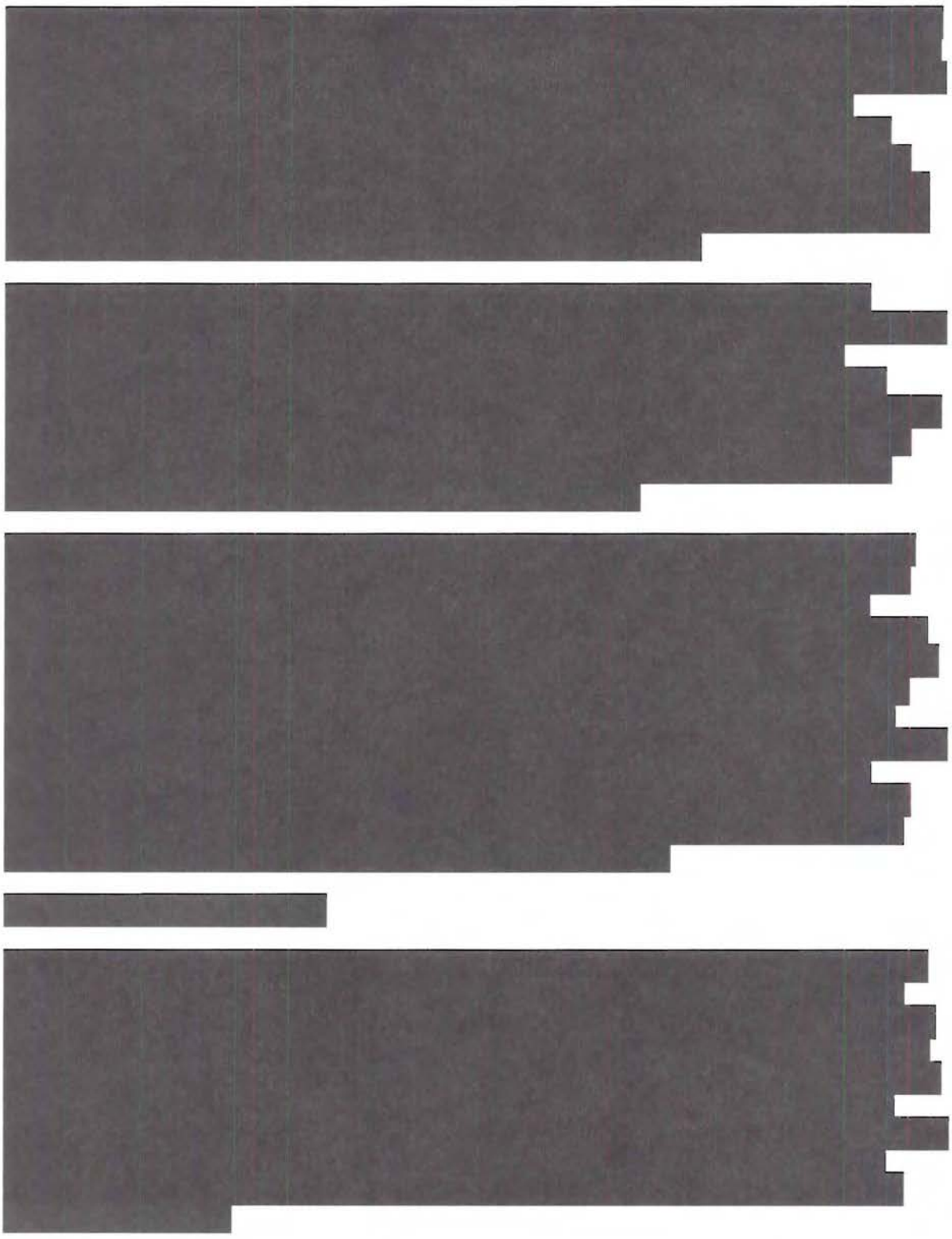
~~(TS//SI//NF)~~ The FISC determined, however, that the minimization procedures governing *retention* of MCTs were inconsistent with the requirements of section 702. The FISC found that the Government had not fully explored options regarding data retention that would be more protective of U.S. persons, and that the FISC thus could not determine that the Government's minimization procedures satisfied FISA's requirement that such procedures be "reasonably designed" to minimize the retention of protected U.S. person information. The FISC further held that, although the Fourth Amendment's warrant requirement was not implicated, in light of NSA's proposed procedures for handling MCTs, NSA's proposed acquisition and minimization procedures did not satisfy the Fourth Amendment's reasonableness requirement. The FISC recognized, however, that the Government may be able to "tailor the scope of NSA's upstream collection, or adopt more stringent post-acquisition safeguards, in a manner that would satisfy the reasonableness requirement of the Fourth Amendment," and suggested a number of possibilities as to how this might be done. *Id.* at 61-63, 78-80.

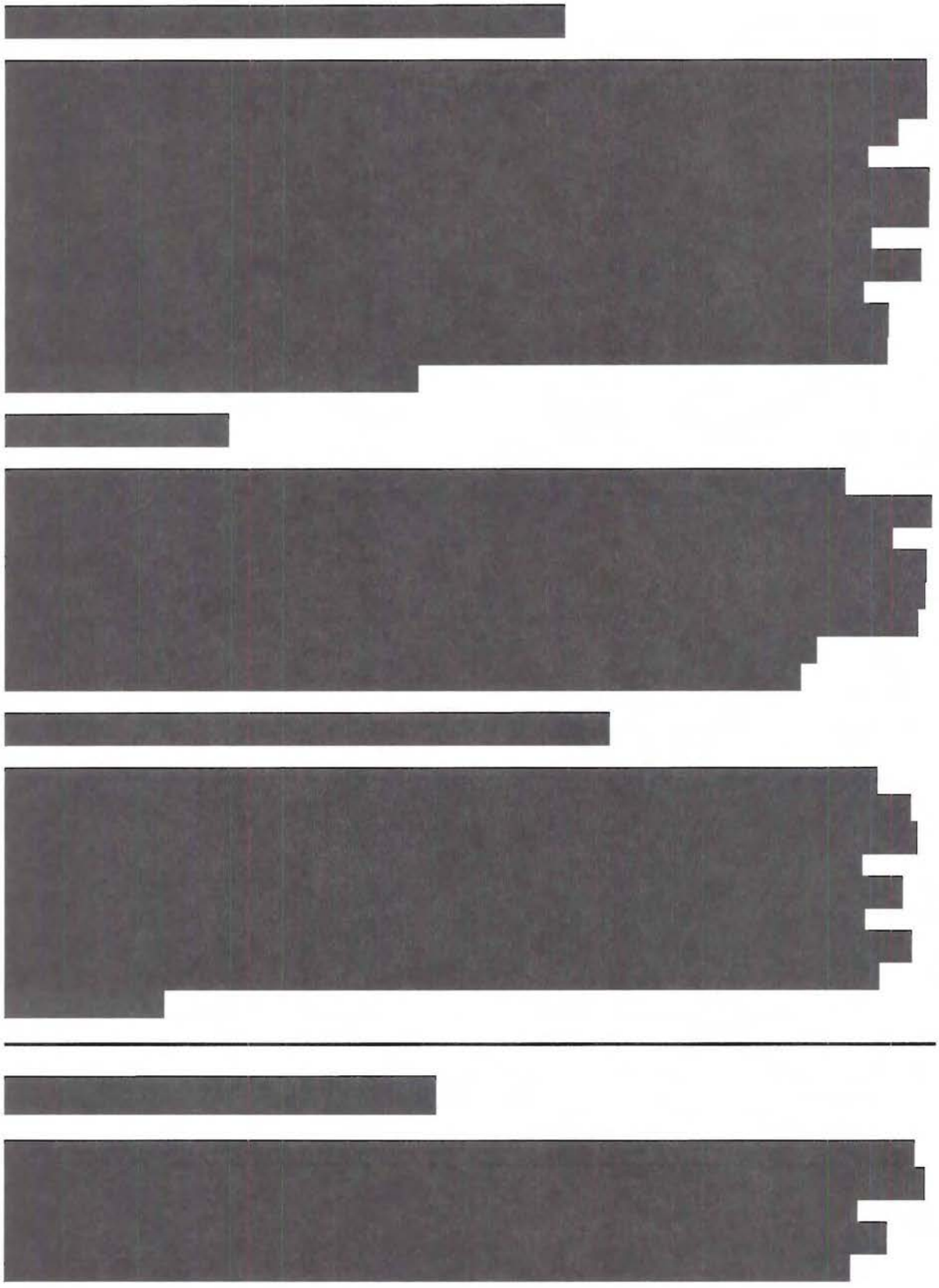
~~(TS//SI//NF)~~ On October 31, 2011, after extensive consultations among the Department, ODNI, and NSA, the Attorney General submitted amended minimization procedures to the FISC addressing the deficiencies noted by the court. These amended procedures continue to allow for the upstream collection of MCTs; however, they also create more rigorous rules governing the retention of MCTs as well as NSA analysts' exposure to, and use of, non-targeted communications. On balance, NSA believes that the impact of these procedures on operations is acceptable as a necessary requirement in order to continue upstream collection, and that these procedures will allow for continued useful intelligence collection and analysis. On November 30, the FISC granted the Government's request for approval of the amended procedures, stating that, with regard to information acquired pursuant to 2011 certifications, "the government has adequately corrected the deficiencies identified in the October 3 Opinion," and that the amended procedures, when "viewed as a whole, meet the applicable statutory and constitutional requirements."

(U) The Government has provided copies of the opinions and the filings by the Government to this Committee, and the Government will continue to inform the Committee about developments in this matter.

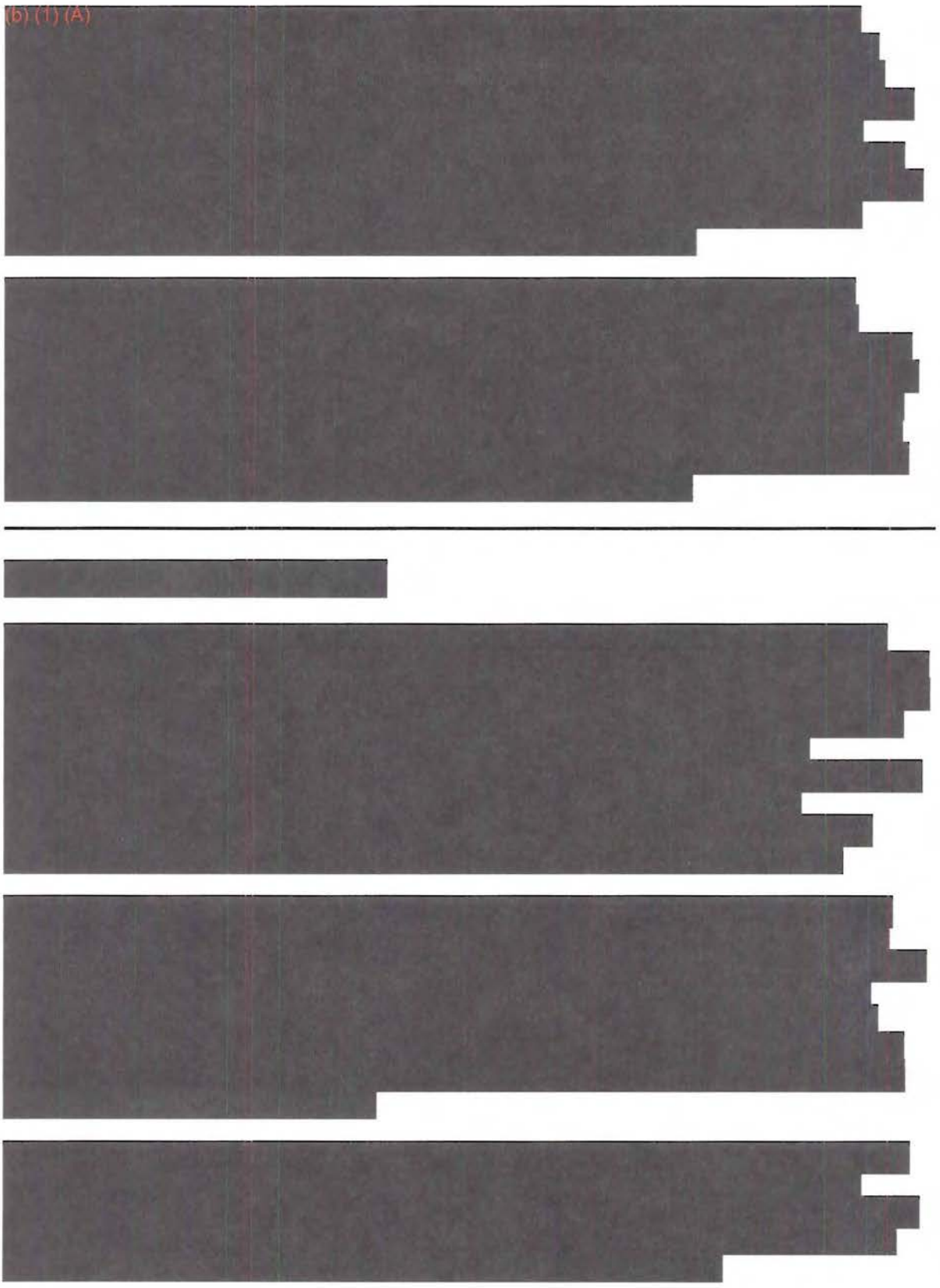


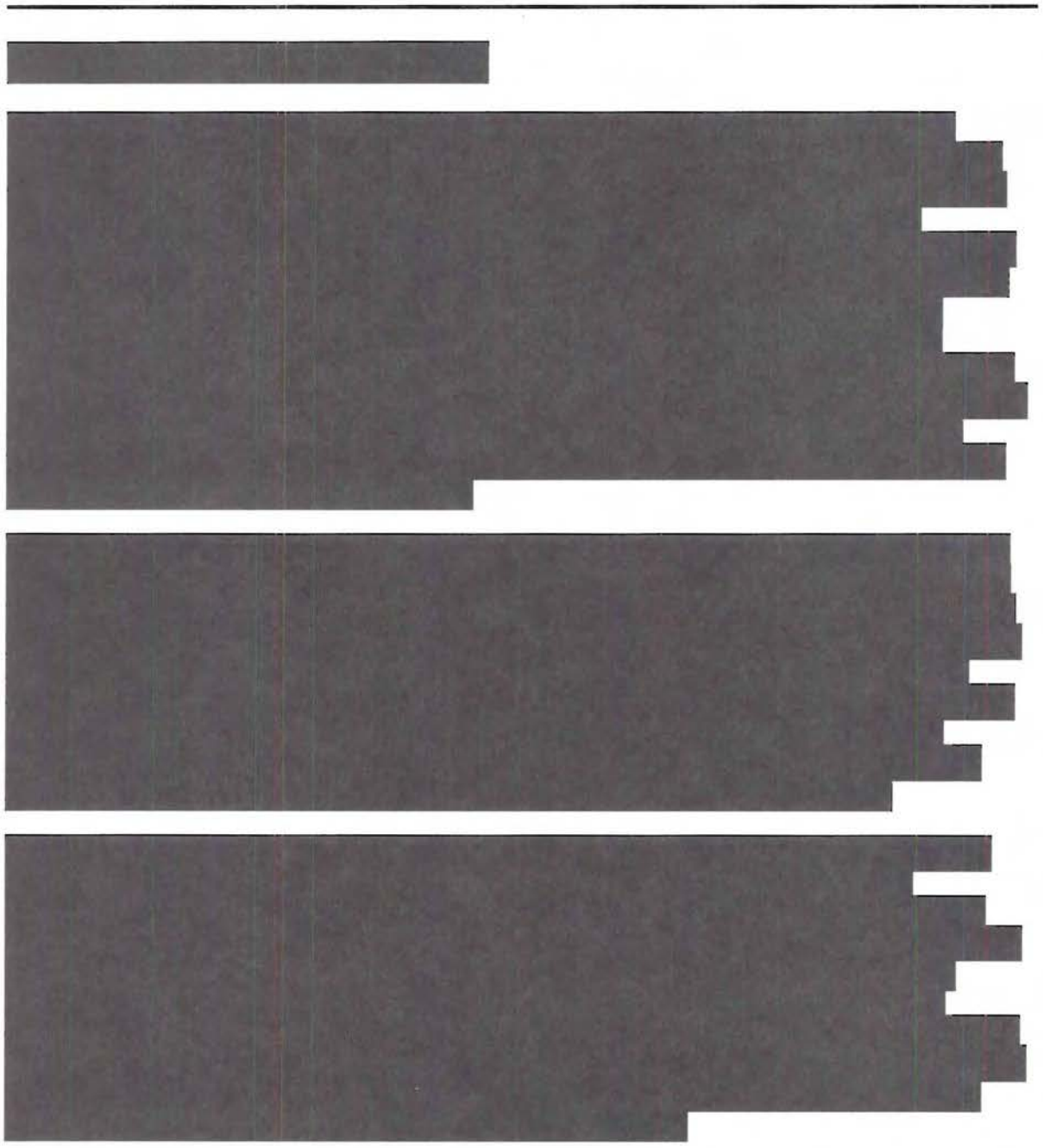






(b) (1) (A)





DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix P

This document was also filed as ECF No. 168-20 and can be found in this Joint Appendix at JA2631.

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix Q

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

Public Hearing Regarding the
Surveillance Program Operated Pursuant to
Section 702 of the Foreign Intelligence
Surveillance Act

March 19, 2014

The public hearing was held at the Renaissance Mayflower Hotel, 1127 Connecticut Avenue NW, Washington, D.C. 20036 commencing at 9:00 a.m.

Reported by: Lynne Livingston

BOARD MEMBERS

David Medine, Chairman
Rachel Brand
Patricia Wald
James Dempsey
Elizabeth Collins Cook

PANEL I

Government Perspective on Section 702 Foreign Intelligence Surveillance Act

James A. Baker, General Counsel, Federal Bureau of Investigations
Rajesh De, General Counsel, National Security Agency
Robert Litt, General Counsel, Office of the Director of National Intelligence
Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, Department of Justice

PANEL II

Legal Issues with 702

Foreign Intelligence Surveillance Act

Laura Donohue, Professor of Law, Georgetown University Law School

Jameel Jaffer, Deputy Legal Director, American Civil Liberties Union

Julian Ku, Professor of Law, Hofstra University

Rachel Levinson-Waldman, Counsel, Liberty and National Security Program, Brennan Center for Justice

PANEL III

Transnational and Policy Issues

John Bellinger, Partner, Arnold and Porter

Dean C. Garfield, President and CEO, Information Technology Industry Council

Laura Pitter, Senior National Security Researcher, Human Rights Watch

Ulrich Sieber, Director, Max Planck Institute for Foreign and International Criminal Law, Germany

Christopher Wolf, Partner, Hogan Lovells

PROCEEDINGS

MR. MEDINE: Good morning. Welcome to the Privacy and Civil Liberties Oversight Board's hearing on the 702 Program.

I'm David Medine, PCLOB's chairman. It's 9:05 a.m. on March 19th, 2014 and we are in the grand ballroom of the Mayflower Hotel located at 1127 Connecticut Avenue, NW, Washington, D.C.

This hearing was announced in the Federal Register on March 10th, 2014. As chairman, I will be the presiding officer.

All five Board members are present and there is a quorum. The Board members are Rachel Brand, Elisebeth Collins Cook, James Dempsey, and Patricia Wald.

I will now call the hearing to order. All in favor of opening the hearing please say aye.

(Aye)

MR. MEDINE: Upon receiving unanimous consent to proceed, we will now proceed.

I want to thank the many panelists who

will be participating in today's hearing for agreeing to share their views with the Board.

I also wanted to thank the Board's staff, Sharon Bradford Franklin, Sue Reingold, Peter Winn, Diane Janosek, Brian Frazelle, and Simone Awang for their efforts in making this event possible.

Last year PCLOB agreed to provide the President and Congress a public report on two federal counterterrorism programs, the Section 215 program under the USA PATRIOT Act and the 702 program under the FISA Amendments Act. The report on the 215 program was issued on January 23rd, 2014.

Our focus today will be on the Section 702 program under the FISA Amendments Act. The purpose of this hearing is to foster a public discussion of legal, constitutional, and policy issues relating to this program.

A few ground rules for today, we expect that the discussion will be based on unclassified or declassified information, however some of the

discussion will inevitably touch on leaked classified documents or media reports of classified information.

In order to promote a robust discussion speakers may choose to reference these documents or information, but they should keep in mind that in some cases they remain classified. Therefore, while discussing them, neither the Board members nor speakers in a position to do so will confirm the validity of the documents or information.

There will be three panels today. The first will consist of government officials whose agencies have varying degrees of responsibility for the surveillance programs that will be the subject of our report.

The second panel with consist of academics and advocates who will focus on legal issues, including statutory and constitutional issues. After the first two panels we will be taking a lunch break.

The final panel will consist of a mix of academics, advocates, and private sector

representatives and will focus on transnational and policy issues.

Board members will each pose questions during each panel with questions in rounds for each Board member. Panelists are urged to keep their responses brief and to permit the greatest exchange of views.

The program is being recorded and a transcript will be posted on PCLOB.gov. Written comments from members of the public are welcome and may be submitted online at regulations.gov or by mail until March 28th.

Today's hearing will focus on the government's collection of foreign intelligence information from electronic communication service providers under court supervision pursuant to Section 702 of the Foreign Intelligence Surveillance Act.

Information is obtained with FISA court approval based on written directives from the Attorney General and the Director of National Intelligence to acquire foreign intelligence

information. This law permits the government to target non-U.S. persons, someone who is not a citizen or a permanent resident alien, located outside the United States for foreign intelligence purposes without obtaining a specific warrant for each target.

We will now turn to our first panel, and I understand that Bob Litt will be making an opening statement for the panel.

MR. LITT: Thank you, and thank you for the opportunity to appear on behalf of the whole group here and talk about Section 702.

I would like to give a brief overview of Section 702 to set the stage, and we'll be glad to fill out some of the points I make here in response to questions.

Section 702, as you noted, enables us to collect intelligence against foreign targets who are outside of the United States while robustly protecting privacy rights.

Under Section 702 the FISA court approves annual certifications submitted by the

Attorney General and the Director of National Intelligence that identify categories of foreign intelligence that may be collected. We then target selectors such as telephone numbers or email addresses that will produce foreign intelligence falling within the scope of the certifications.

The FISA court also has to review and approve targeting and minimization procedures. The targeting procedures ensure that we target only non-U.S. persons who are reasonably believed to be outside of the United States, that we do not intentionally intercept totally domestic communications, and that we do not target any person outside of the United States as a subterfuge to actually target someone inside the U.S.

The minimization procedures ensure that consistent with foreign intelligence needs, we minimize the acquisition and retention of non-public information available about U.S. persons and that we prohibit the dissemination of

such information.

I want to make a couple of important overview points about Section 702. First, there is either a misconception or a mischaracterization commonly repeated that Section 702 is a form of bulk collection. It is not bulk collection. It is targeted collection based on selectors such as telephone numbers or email addresses where there's reason to believe that the selector is relevant to a foreign intelligence purpose.

I just want to repeat that Section 702 is not a bulk collection program.

Second, from a legal point of view persons who are not U.S. persons and who are outside of the United States do not have rights under the Fourth Amendment and so the Constitution doesn't require individualized warrants to target them.

In fact, the type of intelligence that is covered by Section 702 targeting foreigners outside of the United States has historically been viewed as part of the President's inherent

constitutional authority and I'm not aware of any other country that brings this kind of collection under this sort of judicial process.

Third, collection under 702 is subject to extensive oversight by all three branches of government. We can explain the oversight in more detail later, but it includes extensive review of collection activities under Section 702 by inspectors general, by the Department of Justice, and the Office of the Director of National Intelligence. It includes reporting of all compliance incidents to the Foreign Intelligence Surveillance Court, and it includes periodic reports both to Congress and to the court.

As the documents that we've declassified and released make clear, the Foreign Intelligence Surveillance Court carefully scrutinizes our activities under this section. And while there have been a number of compliance incidents over the years, the court has never found any intentional efforts to violate the requirements of Section 702.

Fourth, the fact that the communications of U.S. persons may be incidentally intercepted when we target valid foreign intelligence targets is neither unexpected nor unique to Section 702 collection.

Both the statute itself with its required minimization procedures and the legislative history make completely clear that Congress knew full well when it passed Section 702 that incidental collection of communications of U.S. persons would occur when they're in communication with valid foreign targets.

And it's important to note that this kind of incidental collection occurs all the time in other contexts. When we conduct a criminal wiretap or a wiretap pursuant to Title I of FISA we will likely intercept communications of persons who are not targets. When we seize someone's computer we may find communications with persons who are not targets.

The minimization rules under Section 702 which the FISA court approves is consistent

with both the statute and the Fourth Amendment are designed to protect the privacy of persons whose communications are incidentally collected, while still allowing the use of information that is lawfully collected for valid foreign intelligence and law enforcement purposes.

Finally, I want to close by just emphasizing that Section 702 is one of the most valuable collection tools that we have. Many of the specific achievements of Section 702 have to remain classified so that we aren't revealing exactly who we're targeting and what we're collecting. But it is one of our most important sources of information, not only about terrorism but about a wide variety of other threats to our nation.

And unless one of my colleagues has something to add, I think we're ready to address your questions.

MR. MEDINE: Great, thank you very much for that statement.

I wanted to start off and pick up with

your discussion of incidental collection, and again just to make clear that under this program, even though the target may be a non-U.S. person there will be times when the conversations, either by email or telephone, the person on the other end will be a U.S. person.

And so my question to the panel is whether because you're gathering communications of U.S. persons if that implicates Fourth Amendment concerns? And if so, do you believe there's a foreign intelligence exception to the Fourth Amendment? And if not, how is warrantless collection of information of U.S. persons permissible?

And then to follow up on Mr. Litt's comment analogizing this to a traditional wiretap, is there a distinction here where on a traditional wiretap the court has, there's been a judicial determination with particularity of a particular collection, whereas here there's only broad programmatic court approval and not approval of the specific collection?

So I guess broadly speaking, can you address the Fourth Amendment concerns regarding incidental collection?

MR. WIEGMANN: Sure, I'll take that. So this is, as Bob said, collection that is targeting non-U.S. persons overseas who don't enjoy Fourth Amendment rights under controlling Supreme Court precedent. So that affects the Fourth Amendment analysis.

That's not to say that U.S. persons whose information is or whose communications are collected incidentally doesn't trigger a Fourth Amendment review. It does. Those people still have Fourth Amendment rights, but what the courts have said is that, what the FISA court has said is that the minimization procedures that are in place render that collection reasonable from a Fourth Amendment perspective.

We think there's an exception to the warrant requirement. Before FISA was enacted in the 1970s a number of courts held in a number of different circuits that there is a foreign

intelligence exception to the warrant requirement under the Fourth Amendment, in light of the special needs of the government to collect foreign intelligence, weighed against the privacy interests of U.S. persons concluded that you don't need a warrant when you're engaged in foreign intelligence collection.

So then the only remaining question is, is it reasonable under the Fourth Amendment to collect information on U.S. persons incidentally when you're targeting non-U.S. persons. And what the FISA court has held is that it is reasonable in light of the minimization targeting procedures that we have in place. So I don't know if that answers your question, but.

So the way you look at it is the warrant requirements not applicable to foreign intelligence collection still have a reasonableness requirement with respect to incidentally collected U.S. persons, and that in fact, it is reasonable in light of the procedures that we have that are designed to ensure that we

are targeting only non-U.S. persons.

MR. MEDINE: And could you address why the minimization procedures make it a reasonable form of collection under the Fourth Amendment?

MR. WIEGMANN: Yes, so the minimization procedures address, and the targeting procedures address the acquisition, retention, and dissemination of U.S. person information.

And so those procedures all are designed to protect those U.S. persons whose information might be incidentally collected.

So for example, you can only disseminate information about a U.S. person if it is foreign intelligence, or necessary to understand foreign intelligence, or is evidence of a crime.

You have retention rules. I believe in some cases, for NSA for example, you have a five year retention limit on how long the information can be retained. And so these are procedures that the courts have found protect U.S. privacy and make the collection reasonable for Fourth

Amendment purposes.

MR. MEDINE: And under the minimization procedures I understand that the agency, the NSA, FBI, the CIA have their own minimization procedures and they're not the same with each other?

MR. WIEGMANN: That's right.

MR. MEDINE: Can you address why that shouldn't be a concern that this information is not being subjected to the same minimization standards?

MR. WIEGMANN: So each of them have their own minimization procedures based on their unique mission, and the court reviews each of those for CIA, FBI, NSA, and it's found them all reasonable for each different agency. They're slightly different based on the operational needs, but they're similar.

MR. MEDINE: Would it make more sense then if the same set of minimization procedures apply across the board for this kind of information?

MR. WIEGMANN: I don't think. Again, just to contrast, for example, FBI and NSA that are using information in different ways. The FBI has a little more latitude with respect to U.S. person information in terms of criminal activity and evidence of a crime than NSA, which doesn't have that law enforcement mission. So I think it is important to have some differences between the agencies in terms of how they handle the information.

MR. MEDINE: And is it the practice that all information that's collected under 702 is subject to the minimization procedures?

Some questions I think have been raised in some of the comments that were submitted as to whether address books or other information would be considered communications that would be subject to minimization, or is it the approach that all information collected under 702 is subject to minimization?

MR. WIEGMANN: All U.S. person information is subject to minimization procedures.

MR. MEDINE: I think my time is up.

MS. BRAND: First of all, thanks to all of you for being here this morning. We appreciate your taking the time and making yourselves available.

I want to continue on the Fourth Amendment discussion. Could one of you explain the process both inside the executive branch and then with the court of conducting the Fourth Amendment analysis and seeking the court's approval of the Fourth Amendment analysis and what kinds of opinions on the Fourth Amendment you've had from the court, to the extent that you can talk about it. Help us to understand how that works.

MR. WIEGMANN: So, you know, the FISA court operates a little bit differently than a regular court in the sense that it's ex parte, but. So that means only the government is there. There's not a party on the other side.

But other than that, we are briefing the legal issues in much the same way as we would

in a regular proceeding where there is a party on the other side. So we have an obligation to persuade the court that the collection under 702 is lawful, that it complies with the Fourth Amendment, and as I just explained to the chair, that minimization procedures comply with the Fourth Amendment.

So we would brief that issue explaining the Fourth Amendment procedures, and the court issues opinions and has issued opinions going through the Fourth Amendment analysis and finding that 702 collection, including the minimization targeting procedures meets the Fourth Amendment standards. So it's a full-up kind of regular legal briefing on that.

MR. LITT: And if I could just add something to that, it is typical in matters that involve the collection of evidence for these proceedings to be conducted ex parte. Wiretap or search warrant applications are also all done ex parte, even if they happen to present significant legal issues. So this is nothing novel in terms

of the approach that's taken there.

MR. DE: And if I could have one point. So in addition to what Brad was articulating, the court reviews this at least annually, the Fourth Amendment analysis.

As you all know, the 702 process requires annual certification. As part of that certification process every year the minimization and targeting procedures for the various agencies are submitted to the FISC, which by statute has to conduct a Fourth Amendment analysis on those procedures as part of that annual review process.

MS. BRAND: So the Fourth Amendment analysis is once a year of the program overall?

MR. DE: Well, the court has consistent jurisdiction over the program all year. The point I was making is that as part of the annual certification process, by statute the court is required to do a Fourth Amendment analysis of the annual, of the procedures that are submitted annually.

MR. BAKER: It gets evaluated at least

once a year.

MS. BRAND: Can you elaborate on that? What would there be in addition to that once a year analysis?

MR. DE: There could be a variety of factors. There could be a need to change procedures in the year, so that would prompt another analysis. I don't believe we've done that but that could be one circumstance.

There could be a variety of compliance matters that raise particular concerns to the court, in which case the court may want to do a review off-cycle.

So I think we wouldn't presume and say it only had to be once a year, but at a minimum by statute it needs to be once a year.

MS. BRAND: Okay. Bob, you talked about 702 not being bulk collection. I'd like to delve into that a little bit more, it's not bulk collection. You talked about selectors. We need to elaborate on that a little bit, I think. What is it? It's not bulk you say, but what is it?

MR. LITT: Sure. Well, I think it's probably helpful to talk about what bulk collection is first of all.

And if you look at the President's policy directive there's a definition. I don't have it in front of me, but it's essentially bulk collection is collection of communications without relying on some sort of discriminant to ensure that you're targeting particular collection.

It's sort of viewed sort of more informally, it's getting a whole bunch of communications, hanging onto them and then figuring out later what you want.

This is not that. This is a situation where we figure out what we want and we get that specifically. And so that's why it is targeted collection rather than bulk collection. Is that helpful?

MS. BRAND: But I'd like to get a little bit more into what is it that you're getting. So you have a selector, I mean.

MR. LITT: Sure. So Raj probably can

talk to this a little better than I can.

MR. DE: So if I could, I'd step back and just talk about the different types of collection under Section 702, which I think is a necessary predicate to understand how collection occurs.

So there's two types of collection under Section 702. Both are targeted, as Bob was saying, which means they are both selector-based, and I'll get into some more detail about what that means. Selectors are things like phone numbers and email addresses.

Both are affected by compulsory legal process, both types are conducted with the assistance of electronic communication service providers, and both types of collection under 702 are subject to the same statutory standards, so just as a predicate.

The first type is what's now been come to be known as PRISM collection, so just using that shorthand for a moment. And under this type of collection, communications to or from specific

selectors, again, things like phone numbers or emails, are provided with the assistance of ISPs pursuant to directives.

The second type of collection is the shorthand referred to as upstream collection. Upstream collection refers to collection from the, for lack of a better phrase, Internet backbone rather than Internet service providers.

It is also however selector-based, i.e. based on particular phone numbers or emails, things like phone numbers or emails. This is collection to, from, or about selectors, the same selectors that are used in PRISM selection. This is not collection based on key words, for example.

This type of collection upstream fills a particular gap of allowing us to collect communications that are not available under PRISM collection.

But given the unique nature of upstream collection there are different minimization procedures that apply, to get to the chair's question earlier.

The reason procedures aren't always the same for different types of collection, as Brad articulated, is that there are both different mission interests and different privacy interests at stake.

MS. BRAND: I see my time is up, so.

MS. COLLINS COOK: Thank you for coming here this morning. We really appreciate your time on this and happy to be a part of this dialogue here.

I wanted to follow up on a couple of points that have already been raised, but first, we've talked about the Fourth Amendment implications of the collection. We've also talked about the fact that, or it is known that the information that's collected can subsequently be queried.

Do you consider that subsequent query a search for the purposes of the Fourth Amendment? And if not, why not?

MR. WIEGMANN: No, I would say that the search occurs at the time that the collection

occurs. So when the information, as Raj just explained, from a particular selector is acquired by NSA, then that's the time at which the search occurs.

Once you've lawfully collected that information, subsequently querying that information isn't a search under the Fourth Amendment, it's information already in the government's custody. And so I don't think there are any other contexts really in general in which a warrant is required to search information already in your custody.

MS. COLLINS COOK: Following up on that, I think some have suggested that whether as a matter of Fourth Amendment necessity or as a policy, as a matter of policy that you should seek court approval before doing a query of a U.S. person identifier.

Can you talk a little bit about what the operational impact of such a requirement might be?

MR. WIEGMANN: Sure, and this is

something I guess some of my colleagues could talk about the operational impact. But as I said, in general with other types of collection, whether it's collection under Title I of FISA, which is your regular collection under which you've gone to the FISA court and already gotten approval to target a particular agent of a foreign power in the United States, or moving over to the criminal side if it's information collected under the Wiretap Act, commonly known as Title III, under which you're conducting surveillance, let's say of an organized crime figure or in a drug case of an individual, in all of these contexts we collect information.

We don't, once we've collected it, we've gotten the necessary court approvals to obtain the information, we don't then have to go back to court to query the same information that we've already collected lawfully a second time to say is it okay to look at it. We've already gotten the conclusion that it's legal to collect it.

And if you have to go back to court every time you look at the information in your custody you can imagine that that would be quite burdensome and difficult, to have to go back every time to look at information that's already in your custody. But I can let the FBI and NSA address it a little bit.

MR. DE: If I could add a couple of points and then I'll turn it to my colleague from the bureau.

Just one basic point, we've been talking about U.S. person queries and I just articulated two types of collection. Just to clarify, U.S. person queries are not allowed under what I described as upstream collection. So as I articulated, there may be different reasons to have tailored procedures, minimization procedures for different types of collections. So such queries are not allowed for upstream.

Adding to Brad's point about lawfully collected information, so once information is collected pursuant to 702, the government can and

often will review what it needs to in that information.

Querying that lawfully collected information, one way to think about that is a way to more efficiently review that which the government already has in its possession and can review all of.

And so to get to your question about policy limits on querying that data, one also needs to understand that that information is at the government's disposal to review in the first instance, and querying it is just a way to organize it.

Secondly -- thirdly, if I could add there are standards in place for querying that information, at least for NSA. Such a query, and we're talking about PRISM collection, must be reasonably likely to return foreign intelligence information.

And then finally, in order to disseminate any U.S. person information that may result from such a query it has to be necessary to

understand the foreign intelligence or evidence of a crime is apparent from our publicly available procedures.

But on the operational element, let me turn that to Jim.

MR. BAKER: So just at a high level I think let me make a couple of comments. So first I think you have to think about the fact that you're creating a new and special category of information, as Brad was saying, right. So this would be information that had already been acquired pursuant to lawful process.

We normally will query that. We'll look through that. When something comes in, we'll look through our collected materials to try to find -- a threat comes in, let's say for example. We look at our collected materials, we try to figure out what we have, and then, you know, move forward as expeditiously as possible.

So you would be creating a new category of information that sort of would be off-limits from the normal type of collection that we do.

And I don't pretend to fully understand all the implications that that would have.

But a couple that come to mind, first of all, obviously would be delay. So you would have some additional process that you would have to go through, and I'm sure there would be some kind of emergency carve out and so on, but you'd have to think about and factor in the reality that you would be introducing delay into the system.

You would also then as a result potentially create a gap. There are several types of gaps, I guess. But you would have, there would be a disinclination for people, because either they don't have the facts, or it's just too hard or whatever, to actually go and pursue that extra pot of information.

So there might be some type of connection between what we can look at normally, this material, and then other types of material. And having that type of gap might, you know, actually create a blind spot for us in terms of intelligence collection.

You'd also have to think about, I think, the technical complexity of what it is that you're suggesting. So this is going to have to be segregated in some way, treated differently. And we'd just have to think about that. That could lead to, you know, training issues, technical costs, things like that.

So it's, you just have to actually do it in a way that would be different than from other types of data that we handle, so that's sort of at a high level some of the things that come to mind.

MR. LITT: Beth, can I add one brief point to this which is that over the last decade, decade and a half, there have been a number of commissions that have been set up to investigate after a variety of terrorism incidents, 9/11, Fort Hood, the underwear bomber and so on. Consistently every one of those commissions has found that we need to eliminate barriers to making use of the information that's lawfully in our possession in order to better protect the nation.

And this, requiring some kind of additional process before we can query this information runs directly contrary to the recommendations of all those commissions.

MS. COLLINS COOK: Thank you. I see that my time is up.

MR. MEDINE: By the way, I should say in the excitement of getting into the questioning I never had actually a chance to introduce the panelists. And so I just wanted for the benefit of the audience, you're familiar to us, but for the benefit of the audience we have Jim Baker, who's the General Counsel of the FBI, Raj De, who's the General Counsel at NSA, Bob Litt is the General Counsel at the Director of National Intelligence, and Brad Wiegmann, who is the Deputy Assistant Attorney General at the National Security Division of the Justice Department.

Again, thank you all for being here.

MR. DEMPSEY: Thanks, and thanks to the witnesses for being here. They are very well-known to us. I think everybody should

realize that we've now spent many, many days with these gentlemen and with many, many of their colleagues at all their agencies going through this information, and delving deeply into this.

And there's been a huge amount of dedication of time on the part of the agencies to make sure that we have everything that we ask for and to make sure that all of our questions are answered. And so, you know, all the Board members really appreciate the amount of time that you've dedicated to talking with us.

And I think it is very important here to be one hundred percent clear, and I think there has been a lot of misunderstanding about the 702 program, and I think I do see issues with the program and things we're talking about, but I think it's very important to narrow the subjects of controversy, or discussion, or concern.

And I'm afraid that Raj may have partly reinserted a problem here when you said that U.S. person selectors were not used for upstream collection, or for upstream searches they're not

used at all, period, at the collection stage.

You were saying that U.S. person identifiers or selectors are not used to search the acquired database of communications that were otherwise acquired on a particularized basis under the upstream program, correct?

MR. DE: Correct. I definitely would prefer not to introduce more ambiguities. Let me be absolutely clear, Section 702 collection of any flavor, upstream or PRISM, is only targeting non-U.S. persons reasonably believed to be located abroad.

The topic I was discussing was, is in the realm of that lawfully collected targets information, once it's in the government's possession a secondary issue arises as to how one can search through that data. And the issue that we were discussing was whether those searches can be conducted using U.S. person identifiers within that lawfully data. And the answer to that question is no with respect to upstream collection.

MR. DEMPSEY: And here when you're talking about search and collect and acquire, all of those terms you're using to mean in a colloquial sense when the government collects, obtains, puts into its database, acquires, you're not parsing those words for 702 purposes. There's not a distinction between the search, the collection, the acquisition, right? It's all, you're using those things all that refer to the same activity.

MR. DE: There's no parsing between acquisition or collection.

So there are some theories out there that when the government receives the data it doesn't count as collection or acquisition. That is incorrect. Acquisition and collection for these purposes are the same thing.

But the term search is a different term. Search, as we were just discussing, means searching information that has already been lawfully acquired or collected.

MR. DEMPSEY: Although the first --

okay, so now we have two meanings of search. It's so hard to be clear on this. Brad was explaining a search occurs when you first collect or acquire. That is the Fourth Amendment search.

MR. DE: I think he was speaking to the use of the term in the Fourth Amendment, not the use of the term for purposes of this.

MR. DEMPSEY: And then querying, then there's a second use of search meaning query. So you query your database?

MR. DE: Correct.

MR. LITT: That's the term that we typically use rather than search in that context.

MR. DEMPSEY: Right. In that case a query is not a search for Fourth Amendment purposes.

MR. LITT: Right.

MR. DEMPSEY: Briefly talk a little bit about this 51 percent theory. So persons reasonably believed to be outside the United States, and there's been some talk about, well, so there may have been some slide somewhere, I don't

know where this came from, but some notion that, oh, if it's a 51 percent likelihood, therefore 49 percent of the time we might be wrong, that the person's not outside the United States and that's permitted under 702. Can you comment on that.

MR. DE: Sure. So I think the bigger picture question that that gets to how a determination is made for purposes of the statute that you are in fact targeting a non-U.S. person reasonably believed to be located abroad.

So as Bob articulated, and I'm sorry for repeating this but just for clarity, the statute does not allow us to target U.S. persons, it does not allow the government to target anybody within the U.S., it does not allow for reverse targeting, it does not allow for the intentional collection of wholly domestic communications.

So as to how we establish a reasonable belief that the target is in fact a non-U.S. person reasonably believed to be located abroad, there is no 51 percent rule that if you are 51 percent sure it is a non-U.S. person located

abroad that is sufficient. That is not the rule, and I don't honestly know where that misconception has come from.

The foreignness determination, which is shorthand for referring to the determination that it is a non-U.S. person reasonably located to be abroad, is based on a totality of the circumstances.

So what does that mean? That means that an analyst must take into account all available information. It means that an analyst cannot ignore any contrary information to suggest that that is not the correct status of the person. And it also means naturally that any such determination is very fact-specific to the particular facts at hand.

I did a little checking and it turns out in our internal training materials, at least at NSA, we actually ask our analysts a question along the lines of, if you have four pieces of information that suggests a person is abroad and two pieces of information that suggests a person

is domestic, given that the score is four to two is that sufficient to establish foreignness?

And the correct answer to that is, no, it is not sufficient because it is not a majority test. It is a totality of the circumstances test. One must take into account the strength, credibility, and import of all relevant information.

But just to add on to that, to your bigger point about confidence in that determination, analysts have an affirmative obligation to periodically revisit the foreignness determination. So it is not a once and done system.

Moreover, targeting determinations must be documented ex ante before any collection occurs. That documentation is reviewed, every determination is reviewed in 60 day increments by the Department of Justice and the Office of the Director of National Intelligence to determine if they agree with that determination.

And then finally, the targeting

procedures, as we mentioned, which account for a lot of this are reviewed annually by the Foreign Intelligence Surveillance Court and approved to be consistent with the Fourth Amendment and the statute obviously.

MR. WIEGMANN: And if I could just add from the DOJ perspective, as Raj said, we reviewed all of those foreignness determinations and we found an error rate of less than .1 percent basically. So that equates to essentially less than one in a thousand cases in which we're finding that NSA is making erroneous foreignness determinations.

MR. MEDINE: Judge Wald.

MS. WALD: Thank you again. I think that the NSA has said that in some of its information that if information about U.S. persons is collected incidentally to a 702 search that was targeted on a non-U.S. person and the incidental information about U.S. persons is found not to have any foreign intelligence value it will be, quote, purged.

Can you explain exactly what purging means? Does that mean that it can subsequently not be used at all, or it can be subsequently used or retained for some purposes? And finally, at what point and by whom would this decision of non-intelligence value be made? There's a lot of sub-questions.

MR. DE: Sure. Well, let me step back for a moment. If the information is determined to not have --

MS. WALD: Could you just speak a tiny bit louder because I'm at the tail-end of this table.

MR. DE: Certainly. If information is determined to not have foreign intelligence value then it is required to be purged.

What purging means is removed from NSA systems in a way that it cannot be used, period.

MS. WALD: For any reason at all?

MR. DE: Correct. There are extensive requirements we have gone through with the Foreign Intelligence Surveillance Court to ensure to the

best extent humanly possible that NSA's technical systems can, in fact, purge data as required by both our minimization procedures and the Foreign Intelligence Surveillance Court.

MS. WALD: But just to pursue that a little bit, in your experience is that to purge or not to purge decision made early in the process or is it kept in there until the analyst or whoever has a chance to do some more hunting around and see whether or not maybe other things would suggest that that does have intelligence value?

In other words, if there's such a concern about U.S., as there is in outside groups, about U.S. incidental information that's in the files and later there's a possibility of it being queried, I wonder how extensive this purging operation really is?

MR. DE: To purge or not to purge, that is the question.

MS. WALD: Yes.

MR. DE: So our procedures require that the determination about foreign intelligence value

be made as early as possible in the, what one in the technical sense calls the processing cycle. So it is not something that by default can be ignored.

That being said --

MS. WALD: And who makes that?

MR. DE: An assessment as to foreign intelligence value is made by foreign intelligence analysts.

MS. WALD: By the analysts who are working on it?

MR. DE: Correct, as they would be the ones who have the most relevant information.

But that also goes to a bigger point as to the nature of intelligence analysis. I think you all would appreciate that it's difficult to determine without context the foreign intelligence value of any particular piece of information. In fact, that's why the intelligence community is often encouraged to connect the dots of various pieces of disparate information.

And so I think we would hope and expect

that analysts make that determination about foreign intelligence value within the context of all available information.

But to your point as to if information is not reviewed, what is the default? This is a large reason why we in fact have default retention periods for data. And for example, for NSA the default for PRISM collection is a five year retention period.

But that's also a reason why that retention period is adjustable, or at least is tailored to the specific nature of the collection.

So for example, for upstream collection the retention period is two years, recognizing the nature of, the unique nature of upstream collection and that it may have a greater implication for privacy interests.

MS. WALD: Okay. The President required, I think he required in his January directive that went to 215 that at least temporarily the selectors in 215 for querying the databank of U.S. telephone calls metadata had to

be approved by the FISA court.

Why wouldn't a similar requirement for 702 be appropriate in the case where U.S. person indicators are used to search the PRISM database? I mean what big difference do you see there?

MR. LITT: Well, I think from a theoretical perspective it's the difference between a bulk collection and a targeted collection, which is that the --

MS. WALD: But I would think that, I'm sorry for interrupting, Bob. I would think that message, since 702 has actually got the content.

MR. LITT: Well, and the second point I was going to make is that I think the operational burden in the context of 702 would be far greater than in the context of 215.

If you recall the number of actual telephone numbers as to which a RAS, reasonable articulable suspicion determination was made under Section 215 was very small.

The number of times that we query the 702 database for information is considerably

larger. I suspect that the Foreign Intelligence Surveillance Court would be extremely unhappy if they were required to approve every such query.

MS. WALD: I suppose the ultimate question for us is whether or not the inconvenience to the agencies, or even the unhappiness of the FISA court would be the ultimate criteria.

MR. LITT: Well, I mean I think it's more than a question of inconvenience. I think it's a question of practicability.

MR. DE: And if I could add one point to that. I think one must also look at the underlying nature of the collection program at issue. And so I think we should be clear not to conflate the 215 program with the 702 program, and as you mentioned, one deals with metadata and one deals with content.

But the important point being the latter is directed at content collection targeting non-U.S. persons located abroad, whereas the 215 program, although it deals with metadata, did not

have such a necessary distinction.

MS. WALD: It did have a selective, I mean the 215 program and the original --

MR. MEDINE: I'm going to, your time, the Judge's time has expired, but we'll have an opportunity in another round to continue that discussion.

I want to shift to a different topic, which is about communication, about searches or about queries, which is, and I'm happy to have you explain it, but my understanding basically is that you are looking for other peoples' discussion of a particular selector or email term.

But I'd like to get back to some of the definitions here, which are there are some terms here that would be helpful to understand your view of, which is what is a target? What is a tasking? What is a selector? What's a directive?

If you could explain those terms, because I did want to shift to how those terms might apply in the about context.

MR. WIEGMANN: Okay, I can take a stab

at that. So a target is the -- maybe I should start with selector since that's the operative term that the others build on.

A selector would typically be an email account or a phone number that you are targeting. So this is the, you get, you know, terrorists at Google.com, you know, whatever. That's the address that you have information about that if you have reason to believe that that person is a terrorist and you would like to collect foreign intelligence information, I might be focusing on that person's account.

So when you go up on that selector, we say go up on or target that selector, that means we're collecting information, we're going to the provider and getting information related to that person's account.

So we're intercepting in real time and then collecting the historic communications of that particular account.

Okay, so that's what we mean by targeting a selector. You're using that selector,

you're providing that to the company, the provider, to get information on that account, or if it's a phone number on that phone number.

So that's when we say selector it's really an arcane term that people wouldn't understand, but it's really phone numbers, email addresses, things like that.

And targeting, it means that's the one you're trying to get. They may be in communication with other email addresses or other phone numbers and so forth. Those are not the targeted numbers or accounts, those are others that are incidentally acquired because they're on the other end of these communications. So target is the one you're going after.

And the statute requires that that target be a non-U.S. person located overseas. And so that's the foreignness determinations that we're talking about as we go through at great lengths to make sure that that target is in fact belongs to a non-U.S. person that is located overseas.

The other two questions?

MR. MEDINE: Tasking or task.

MR. WIEGMANN: Tasking is when you're going and saying, okay, I want to task this account means I want to collect information from that account. So that's the collection.

MR. LITT: You task a selector.

MR. WIEGMANN: You task a selector. So you're identifying, that's when you take that selector to the company and say this one's been approved. You've concluded that it is, does belong to a non-U.S. person overseas, a terrorist, or a proliferator, or a cyber person, right, whoever it is, and then we go to the company and get the information.

MR. MEDINE: And directives.

MR. WIEGMANN: So directives are the orders that go to the companies that say they have to comply with the lawful tasking. So that's the kind of more overarching order that goes to a company provider and says, okay, you have a legal obligation to comply with the taskings that are

given to you and here are the rules and everything. And that's all provided to them.

Is that a fair summary? I'll ask my colleagues to see if that is --

MR. DE: Keeping target as the statutory term. A term like selector is just an operational term to refer to something like an email or phone number, directive being the legal process by which that's effectuated, and tasking being the sort of internal government term for how you start the collection on a particular selector.

MR. MEDINE: Okay. So I guess building on that, what's the statutory rationale for about collections, because if the target is the email account or phone number, what is the justification for gathering communications between two persons, it may even be two U.S. persons who are discussing that phone number or that email address, but they are not themselves, there's no to or from that particular email address or particular phone number, why is that targeting that is permissible under the statute?

MR. WIEGMANN: Right. So the conclusion there again in a typical case, you're right, if you're targeting, you know, bad guy at Google.com you're targeting that person's accounts, their communications.

Why abouts collection is different is it's not necessarily communications to or from that bad guy but instead about that selector.

And so what the court has concluded is that when the statute uses the term targeting of a non-U.S. person overseas, targeting that selector qualifies under the statute for targeting that non-U.S. person overseas.

So it doesn't have to be targeting necessarily to or from, but can also target the communications that are about that particular selector.

MR. MEDINE: So that's a different meaning of target than earlier, which is where you're focusing on an account, now you're discussing targeting means discussions about that account.

MR. WIEGMANN: About that selector, correct.

MR. DE: It is always focused on that account, so I think the key is, the misperception that some may have that about collection is somehow about a key word or about the person that may be behind that account.

But all collections under Section 702, whether it's upstream abouts, which is a subset of upstream, or PRISM is all based on the selectors at issue.

MR. MEDINE: But does it raise -- oh, I see my time has expired so I'll --

MS. BRAND: I'm glad to see you're following your own rules.

Just to follow-up on that because that's a good line of inquiry, just to make sure that everyone understands. So you're saying that if someone is emailing about Rachel Brand or about explosives that would not be a permissible about query under your explanation?

MR. DE: So I would like to --

MS. BRAND: But you could, you could perhaps get it about Rachel Brand at --

MR. DE: Just so that, because I think this is an issue that all of us slip into, clarifying querying for collection.

So we are discussing now the collection of information. Abouts is a type of collection of information.

MS. BRAND: I'm sorry, right. Yes, that's right.

MR. DE: And so all collection of information is based, focused on selectors, not key words, as you just mentioned like terrorist, or like a generic name or things along those lines.

MS. BRAND: Okay.

MR. DE: And it's the same selectors that are used for the PRISM program that are also used for upstream collection. It's just a different way to effectuate the collection.

MS. BRAND: Okay. I think a large part of the function of these hearings is a public

education function and so I thought David's questions were great to explain the meaning of different terms, and I'm glad that you're willing to bear with us asking you some questions that we've already discussed with you in private. But I think it's helpful for everyone to understand what we're talking about.

And along those lines there was some discussion in Pat's questions about purging data that doesn't turn out to be foreign intelligence information.

But can you explain how on the front-end you implement the requirement that, not only that the target be a non-U.S. person reasonably believed to be abroad but that you expect to get foreign intelligence information through the collection, that's a separate statutory requirement. How do you go about ensuring that you're collecting that type of information?

MR. DE: Sure. So in our earlier discussion we skipped right to the foreignness determination, but that's actually a second step.

There has to be a reason one actually wants to collect intelligence from the particular selector in the first place.

And then one has to get to the fact, is this a type of collection permitted under the statute? So there has to be a valid foreign intelligence reason to do that collection.

But beyond that there has to be a valid foreign intelligence reason within the ambit of one of those certifications that the FISC approves annually. Those are certifications on things like counterterrorism, encountering WMDs, for example, weapons of mass destruction.

And so when an analyst needs to make a determination as to the valid foreign intelligence purpose for which they want to effectuate collections, they must also document that.

That is documented in a targeting rationale document in advance, ex ante, and those are always reviewed by the Justice Department and the Director of National Intelligence every 60 days.

MR. WIEGMANN: This is an important point for non-U.S. persons because people think about, okay, well once you've concluded that it's a non-U.S. person overseas then you can collect whatever you want. As Raj said, that's really not the case.

It really is targeted, not only based on the identity of the person and the location of the person, but also that you're trying to get foreign intelligence. And so it's an important protection really in the statute that is designed for non-U.S. persons. It's not blanket collection of any non-U.S. person overseas. It's aimed at only those people who are foreign intelligence targets and you have reason to believe that going up on that account that I mentioned, bad guy at Google.com is going to give you back information, information that is foreign intelligence, like on cyber threats, on terrorists, on proliferation, whatever it might be.

MS. BRAND: What can you tell us in an unclassified setting about the documentation of

foreign intelligence purpose or the oversight to ensure? I mean we've talked a little bit about that in past questions, but can you give us anything more specific?

MR. WIEGMANN: They do have to document that at NSA and every -- it's essentially called a tasking sheet, I think. And on that sheet they are documenting the foreign intelligence purpose that they are trying to pursue in going after a particular target.

And those are all reviewed together with the foreignness determination by the Department of Justice on a regular basis.

MS. BRAND: That's a separate sheet for every selector?

MR. WIEGMANN: For every single one, that's right.

MR. BAKER: And I think, at least with respect to FBI, I think the review that Raj mentioned earlier is done every 30 days on these tasking decisions, I guess you'd say, the foreign intelligence and the foreignness determination.

MR. DE: And if I could put that into the broader context of if the question really is getting at what is the process within which that happens, even before that happens we have training for analysts as to how they should document this material, we have audits of our databases, we have a comprehensive compliance program, we have spot checks, even within NSA prior to the 60 day reviews that are done by the Department of Justice and DNI, for us anyway.

There are also quarterly reports to the FISC on compliance with the program, semiannual reports to the FISC and to Congress, and annual inspectors general assessments, and as I mentioned, the annual certification process by the FISC.

So I think those decisions are, while they're one very granular aspect of the program, are conducted within the context of this broader regime.

MS. BRAND: Okay. And I see that my time just ran out.

MS. COLLINS COOK: I wanted to ask one additional question about abouts. Can you do about collection through PRISM?

MR. DE: No.

MS. COLLINS COOK: So it is limited to upstream collection?

MR. DE: Correct. PRISM is only collection to or from selectors.

MS. COLLINS COOK: I wanted to shift to a separate topic. One of the things that I have found both concerning and frustrating through the process of our evaluation of programs is how to both assess and articulate the efficacy of these programs.

And Mr. Litt, you had begun speaking about this in your prepared remarks. And I'd like to ask a couple of questions. One, how do you assess the efficacy of a particular program? How do you think we should be assessing the efficacy of a particular program?

And three, it's not really a question, it's more of a comment which is, please don't give

me a series of success stories and then say that's how you evaluate the efficacy of the program. Because I think that's an initial response from the government often in response to a question, either from a body like ours or from the media.

But how do you assess the efficacy of the program, how periodically do you do so, and how would you encourage us to assess the efficacy?

MR. LITT: Well, let me start on that, and I want to start by saying that I completely agree with you that sort of individual success stories are not the way to evaluate a collection program and its utility.

The way you evaluate collection programs is going to depend in part on what the particular program is for.

In this case, we have in fact the Office of the Director of National Intelligence has attempted, part of our job is to try to determine that resources are effectively allocated within the intelligence community budget.

And so we have done studies to try to

look at, okay, what are our collection priorities, how much reporting is generated on these priorities, and where do those reports come from, what kind of collection source, to the extent we can identify that. And that's one of the ways that we've determined that Section 702 is relevant.

Another thing is just by looking at the sheer nature of the information that we get and its utility towards a whole variety of national priorities. That's a more impressionistic approach, and yet you can see time and again in important intelligence reports that are provided to policy makers that it's derived from Section 702 collection.

So those are two ways that I would look at estimating the value of a particular collection.

MR. DE: If I could just add on to that. With respect to this program or any program I think intelligence professionals will tell you that any tool must be evaluated in the context of

the other tools in which it is utilized.

All intelligence tools are used in complementary fashion with one another and to isolate one particular tool and evaluate its effectiveness in isolation probably doesn't do us justice as to what's valuable and what's not.

It also depends on the type of tool. Different types of intelligence programs are used for different purposes. A program like Section 702 is used for different purposes, for example, than a program, a metadata program with telephony metadata.

One may be a discovery tool to help pursue more specific collection and others may be used as in fact the specific collection that follows from that.

Third, there may be uses in which the PCLOB has recognized in terms of either directing the government in certain directions or at least helping to shape the focus of the government.

And so I think the absolute wrong question is how many plots did this tool stop.

And you can fill in the blank for what this tool refers to. But that is absolutely the wrong question, and I think it won't do us justice to figure out what we need as a government.

MS. COLLINS COOK: I have time I think for one last question. What is the view of the various agencies as to whether or not 702 is an effective and valuable program for the United States?

MR. BAKER: I think it is an effective and valuable program for the United States.

And if I could just address your last question as well. I mean I think you really, in order to understand whether it's effective and useful you have to think about what your goals are with respect to this particular program.

And the goals for this program, like many other collection programs are to obtain I think timely, accurate, informative foreign intelligence information about the capabilities, plans, intentions of foreign powers, agents, actors, and so on and so forth.

And so I think really what you're talking really is, I think, developing a good metric to understand whether this program is worth all of the costs associated with it. And so I think you'd want to look at the amount of information that you, that we acquire, but also then obviously the quality of it. How good is it? And I think you can slice that a lot of different ways, as my colleagues have suggested.

So I think that's really what I would recommend you be focused on. But you have to, because this is a broad-based foreign intelligence collection program you have to look at not only, I mean you have to look at counterterrorism but you have to look more broadly than that because this program is not limited just to counterterrorism.

MR. DE: I agree it's definitely an effective program. I think the one point I should have added is that the review that Bob mentioned happening within the executive branch is not limited to the executive branch.

Congress also reviews the effectiveness

of this program, as well as the 215 program. And I think that's part of the rationale behind having sunset clauses for various programs is that when those statutory provisions expire, as did the 215 program twice in the last five years and as did 702 in 2012, Congress undertakes, as it should, an evaluation of the effectiveness of the programs.

MR. LITT: So I completely agree that it is an effective and important program and I really want to emphasize the last point that Jim made, which is that this program should not be considered solely as a counterterrorism program. This program has utility, has significant and exceedingly important utility in areas outside of counterterrorism.

MR. DEMPSEY: Trying to clear up another issue in terms of the participation of service providers and the awareness of service providers in the 702 implementation, is 702 implemented, all 702 implementation is done with the full knowledge and assistance of any company that, from which information is obtained, is that

correct?

MR. BAKER: Yes. The answer to that is yes.

MR. DEMPSEY: So early on in the debate there were some statements by companies who may or may not have been involved in the program saying, well, we've never heard of PRISM. But whether they ever heard of PRISM, any company that was, from whom information was being obtained under 702 knew that it was being obtained?

MR. LITT: Correct.

MR. DE: PRISM is just an internal government term that as a result of the leaks became a public term. But collection under this program is done pursuant to compulsory legal process that any recipient company would have received.

MR. DEMPSEY: So they know that their data is being obtained because --

MR. DE: They would have received legal process in order to assist the government, yes.

MR. DEMPSEY: One thing I read in one of the statements is under 702 you could target entire countries or regions, is that correct?

MR. DE: So all collection under 702 is based on specific selectors, things like phone numbers or email addresses. It is not a bulk collection program.

MR. DEMPSEY: And a selector would not be an entire area code, for example?

MR. DE: Correct, correct.

MR. DEMPSEY: Going back to the constitutional -- oh, one other set of questions.

Even I've lost track now of what you've already said here versus what you've said elsewhere. But in terms of where you make a determination that a person is a non-U.S. person outside, reasonably believed to be outside the United States and then you later discover that that was good faith but wrong, the person was in United States, or the person was a U.S. person, do you track that, and what do you do when you discover that, and how often do you discover?

I'm not talking about the roamings, I'm talking just about you thought he was outside the United States and that was just wrong, or you thought he was a non-U.S. person and that was just wrong, how often does that occur?

MR. DE: So I'll defer to Brad on the sort of overarching review, but if I could just make a point about what happens. So yes, we keep track of every time new information comes to our attention to suggest that a prior intelligence evaluation was incorrect, even if it had met the legal standard.

Every such incident is a compliance matter that has to be reported to the FISC and ultimately in semiannual reports reported to the Congress.

And third, that sets in process a purging process by which information that should not have been collected if it had not met the legal standard needs to be purged from NSA systems.

I think Brad can speak to the level of

accuracy of those.

MR. BAKER: Just real quick, it's the same. The item is de-tasked and the information is purged.

MR. WIEGMANN: Right. So just to distinguish again between two different types of compliance issues. One is the roamer example that you mentioned.

So this is, let's say we're up on a cell phone that we believe belongs to a bad guy who's outside the United States, a foreign person, and then that person shows up in Chicago, when that happens we de-task that cell phone. That means we're no longer collecting the communications.

That's a compliance incident that's reported but it's not an erroneous determination. It's based on the movement of the individual.

So putting those cases aside, in cases where we just kind of get it wrong, we think the email account or the phone is located overseas but it turns out that that's wrong, or it turns out

that we think it's a non-U.S. person but it is a U.S. person, we do review every single one to see if that's the case.

And our review at Justice we decided to review, and as I mentioned earlier, we think it's less than one in a thousand cases where they make that determination erroneously.

MR. DE: And this probably bears worth repeating that the initial determination is not a once and done, so there is an affirmative obligation for analysts to reaffirm the foreignness determination on a periodic basis, which contributes to the ability to make sure that determination is in fact fresh and current, which of course contributes to the accuracy of that determination.

MR. DEMPSEY: Going to the constitutional issues, back to those for a second, the FISA court has determined, I mean they must they must determine every year that the program is being implemented consistent with the Fourth Amendment.

The very first time they determined that, there was an opinion that they issued. That one is, am I right, not yet public?

MR. WIEGMANN: I think that's correct.

MR. DEMPSEY: Isn't that a good candidate for declassification?

MR. LITT: We have a lot of good candidates for declassification.

MR. DEMPSEY: Yeah.

MR. LITT: In all seriousness there, we are, there are a lot of documents that we have that we are reviewing for declassification that include not only FISA court opinions but a whole variety of other documents.

MR. DEMPSEY: The FISA court in 2008 when they last considered the constitutionality of a program, the predecessor to 702, the court issued a redacted but largely unclassified opinion conducting a relatively full Fourth Amendment analysis.

And there's been some Fourth Amendment analysis conducted in this situation, and if

you're sort of talking about, you know, the Rosetta Stone kind of Ur document, then the very first court opinion should have been the most fulsome explanation of the constitutionality of the program.

I think that -- I mean I hear Bob saying there's a lot of opinions out there, but to me this one seems to be one that would explicate at least one court's judgement on this because it's been the basis of -- I assume all the rest just said nothing has changed that would merit us to reconsider our very first judgement.

MR. WIEGMANN: So I mean I think it's among the opinions. We're committed to reviewing all the opinions of the FISA court to determine which ones can be declassified in redacted form. So I imagine this will be among those that are reviewed. So absolutely, I don't disagree. It'll be among the opinions that will be reviewed.

MR. DE: I just don't want to leave folks with any mysterious misimpression. I think the Board has access to everything and so one

shouldn't have to assume anything about subsequent opinions. The Board has in fact reviewed everything.

And so I just don't want -- what I think would be an unfortunate consequence would be for folks to take away the impression that there is a mysterious opinion that has some secret analysis, and I don't think that's the case. I don't think you intended to suggest that.

MR. MEDINE: The Board does have access to it but I think the question is whether the public should have access to it as part of the debate. But it's Judge Wald's --

MR. DEMPSEY: The public had access to the 2008 --

MR. MEDINE: It's Judge Wald's turn.

MR. WIEGMANN: So just one other thing I would add on that is that 702 collection has now been challenged by a number of criminal defendants when 702 information is being used against them in their cases. And so we'll be filing public briefs and we can expect some more decisions in that area

as well.

So that's another way that the constitutionality of 702 will now be on the public record, or I mean the opinions on it, and the briefs and everything will now be a matter of public record.

MR. MEDINE: Judge Wald.

MS. WALD: Okay. By whom and under what substantive criteria is the initial decision to use a U.S. person selector for searching the PRISM base made? I mean who decides let's do that? What's the substantive criteria on which they make it?

You don't have to go into the review process. I know the decision will be reviewed up and down. But how does that get made? What's the substantive basis?

MR. DE: So I can speak for NSA in particular.

MS. WALD: So just to clarify, that means if it goes to one of the other agencies, not NSA, CIA or FBI or something, they make their own

substantive decisions for querying?

MR. DE: Yes. The 702 program perhaps as a necessary predicate is one that all agencies operate on their own and have their own minimization procedures which would address topics like searches.

NSA's procedures in this regard, in this element have been made public and so the standard is that such a query needs to be reasonably likely to return foreign intelligence information.

MS. WALD: Be reasonably likely. And who is it made by initially?

MR. DE: It's made by the analyst.

MS. WALD: By the analyst who's working on that particular case, okay.

My other question is that the President did, if I understand his directive correctly, direct that there be some changes in the treatment of non-U.S. persons as to the limits on and retention of the data acquired incidentally to bring them more in line with those of U.S. persons

incidentally where there is no foreign intelligence value apparently.

Can you tell us a little bit more specifically if anything has been done in that regard or is being contemplated vis-a-vis 702?

MR. LITT: So I think first of all it's important to understand the point that somebody made, it may have been Brad made earlier, which is that there are already protections to some degree built into the system there. The protections for non-U.S. persons are not as great as those for U.S. persons because U.S. persons are protected by the Fourth Amendment.

But there is a requirement that we can't target a selector unless we have reason to believe it's of foreign intelligence value. And there's sort of a general principle that the intelligence agencies, their job is to collect, analyze, and disseminate foreign intelligence information, not random information.

I think what the President has directed is that we go back and look at our procedures and

not only with respect to 702, but with respect to signals intelligence in general, assess whether, the extent to which it's possible to provide limitations on collection, retention, and dissemination that more closely track those for U.S. persons.

For example, Executive Order 12333 provides specific categories of personal information about U.S. persons that can appropriately be retained and disseminated.

There's a list of them in Executive Order 12333 and the President has asked that we assess whether we can apply those same sorts of rules to personal identifiable information of non-U.S. persons.

MS. WALD: Right now, just to follow-up, right now if you get incidental information about a foreign person in the course of targeting another foreign person and you look at it, do you use the same criteria and look at the same review and say, well, you know, he was just talking to his grandmother or something, there isn't any

foreign intelligence there, and you purge it?

MR. DE: Any time there is not foreign intelligence value to collection, by definition it would be purged.

But I think an important point to be made as you are articulating, Judge, is incidental collection, just to explain that term a little bit, all communications obviously have two ends. One end is the target and the other is presumably not a target. We don't know. One doesn't know ex ante.

And so by definition there will be incidental collection of non-U.S. persons, as well as U.S. persons. Historically, constitutional protections obviously have only applied to the U.S. person subset.

MS. WALD: I understand.

MR. BAKER: Can I just make a comment about that?

MS. WALD: We don't have time. Okay, quickly on the last time, I found it very provocative when you were answering Beth Cook's

question about if you're going to assess the efficacy of a program you have to look at it in terms of its efficacy and the holistic view of all of the programs.

I guess it's inevitable that I would ask the question, but how can anybody except you people do that, because so many of your programs, I think, are just unknown, even to the FISA court? They're not all FISA supervised, and certainly the outside world doesn't know about many of them. So you know, how in effect can an outside assessment be made?

MR. DE: If I could just address it since it was in response to my comment. Certainly I think I would not suggest that there should be a public evaluation of all intelligence programs. I think, for example, this Board as access to information about counterterrorism programs and so I would expect that any evaluation would be in the context of the other CT programs that you have the jurisdiction to review.

As with Congress, as I mentioned, they

reevaluate programs on a periodic basis. And I think the public record now indicates that there is a fairly robust exchange between the executive branch and the legislative branch on a variety of programs. And so I think that's where traditionally the evaluation has occurred.

MR. LITT: Yeah, I was just going to say that we've managed, we've set the balance between public disclosure and the need for secrecy by empowering the congressional intelligence committees. We're required by statute to keep them fully and currently informed of intelligence activities, and we do. They know about these programs and they have the opportunity to evaluate them, and they do.

In fact, they passed an Intelligence Authorization Act that includes a lengthy classified annex that is very prescriptive with respect both to reports that it requires of us and directions as to what we should, you know, where we should be spending our money.

So that's sort of the external

oversight and the way we've said, okay, well, we need to have oversight of these but they still need to remain classified.

MR. MEDINE: Did you want to finish? I don't know, you wanted to make a point earlier about foreign intelligence.

MR. BAKER: I had several points I wanted to make. But let me just on that real quick, I mean I think the, even the addition of Congress having oversight of it, the courts in certain circumstances, and then also obviously the President and all of the executive branch officials, we have an obligation to make sure that in addition to adherence to the law and taking care that the laws are faithfully executed, to spend our time and spend our money on programs that are effective and not be wasting our time on things that are not.

I mean that flows from the President to the DNI, the Attorney General, Director of the FBI, Director of NSA and so on. We should be focused on things that are useful and collecting

information that produces the kind of intelligence information that I was talking about before.

So the other comment that I just wanted to make was just with respect to FBI, our personnel only have access to the databases when they've received the proper training with appropriate oversight and operating consistent with the court-approved standard minimization procedures when they're doing their query activity.

MR. MEDINE: I wanted to shift to a different subject, which is attorney client privilege. There were some press reports a couple of weeks ago about collection of information that may involve attorney client communications.

But I want to focus particularly on the NSA minimization procedures, which I understand do exclude attorney client communications but only in a very narrow context where the client is under criminal indictment and the United States, basically on a federal criminal indictment.

That seems like a very narrow

interpretation of attorney client privilege. I wanted to see if that is the interpretation you apply in minimizing communications, and if it is what impact there would be if it was expanded to the more normally accepted definition of attorney client privilege, which is basically lawyers and clients consulting with each other?

MR. DE: So we have written a letter to the ABA and commented on it to the Board and to the public, I think it's a public letter now, which explicates in fuller detail than I probably can off the top of my head as to our procedures.

But I think one fundamental premise is that analysts are under an obligation to identify for the Office of General Counsel any time they encounter something that may be potentially privileged.

And I think as all of us who are lawyers, I think that probably encompasses every one up here on the stage, knows just because a communication is with a lawyer does not mean it is in fact a privileged communication. So it's

helpful to have a lawyer involved to determine that.

While I can't speak to any particular incident that may have been written about in the press I think there's a couple of big picture points that are worth making. One is our office has historically provided a range of advice to minimize to the extent possible the collection of attorney privileged material.

MR. MEDINE: That's privilege just where there's a criminal indictment or are you viewing privilege --

MR. DE: Beyond the criminal. So the point I'm trying to make is that while there may be a specific provision in the 702 procedures that addresses the criminal context, there's a reason why we ask analysts to consult counsel, because the advice can often be tailored to the specifics of a circumstance far outside the criminal realm, recognizing the import of attorney client privileged material in context, even outside the criminal context.

MR. MEDINE: I want to talk a little bit about reverse targeting where you target someone overseas potentially with the view of collecting information about a U.S. person in the United States, and that's impermissible.

There seems, again maybe this is a somewhat technical point, but there seems to be somewhat of a quirk in the statute. It says that you can target people reasonably believed to be outside the Unites States, you cannot reverse target someone outside the United States if the purpose is to target a particular known person reasonably believed to be in the United States.

Does that permit targeting a person outside the United States with the intent of gathering information about U.S. persons not in the United States?

MR. WIEGMANN: No.

MR. MEDINE: Why not?

MR. WIEGMANN: There's a separate provision that bars targeting U.S. persons outside the United States and so if you were doing that

and you are trying to target a U.S. person outside the United States, you couldn't do that.

MR. MEDINE: So you wouldn't do the reverse targeting procedure?

MR. WIEGMANN: I don't know if you would call that reverse targeting --

MR. DE: There is another statutory provision that prohibits the targeting of U.S. persons outside the U.S. under 702 --

MR. MEDINE: Even reverse targeting? Again, I'm not talking about -- I agree it's clear that you can't target a U.S. person outside of the United States, but what if I find a non-U.S. person that I know is in communication with a U.S. person who's also outside of the United States, is that permissible?

MR. WIEGMANN: No.

MR. DE: No.

MR. MEDINE: Because?

MR. WIEGMANN: Because you would be targeting, if your real purpose is to target that U.S. person, you're targeting that person.

MR. MEDINE: So reverse targeting in your view is the same as targeting? The prohibition on reverse targeting is co-existent with the prohibition on targeting?

MR. WIEGMANN: Well, I mean again I think of reverse targeting as a geographic issue essentially when you're targeting, let's say you have a legitimate target overseas but you really want the communications of a U.S. person or a non-U.S. person inside the United States, but the statute says you can't do that.

MR. MEDINE: Right, but --

MR. WIEGMANN: But as we were just explaining which is if you have a U.S. person that you're interested in overseas, you can't use 702 to target them either and I don't think --

MR. MEDINE: Or reverse target them?

MR. WIEGMANN: What's that?

MR. MEDINE: If you know that that U.S. person is in communication with a non-U.S. person and both of them are overseas --

MR. WIEGMANN: Right.

MR. MEDINE: Could you target the non-U.S. person to get the U.S. person's communications?

MR. WIEGMANN: You couldn't do it for that purpose but if the non-U.S. person overseas is a valid foreign intelligence target that you're interested in their communications, sure, you can target that person. And the fact that they're incidentally communicating with a U.S. person overseas, that's okay. I wouldn't consider that reverse targeting.

You still have to have that legitimate target. I don't know if that answers your question, but.

MR. MEDINE: It did.

MR. BAKER: I'm not going to read it now and take up your time, but take a look at Section 704 A 2, and that may address the kind of concern that you're focused on perhaps, but perhaps not.

MR. MEDINE: Okay. I wanted to get back to efficacy. As you know, our charge is to

look at the balance between national security and privacy and civil liberties, and I think following up on Ms. Cook's question -- sorry, I'll just hold that until the next round.

MS. BRAND: I wanted to go back to upstream collection a little bit. I've seen some statements in the public domain about the volume of upstream collection vis-a-vis the volume of PRISM collection. What can you tell us in a public setting about that?

MR. DE: I think the best publicly available information is from the October 11th, 2011 opinion that has now been declassified in which there was a rough estimate there, and forgive me for if it's not precise, but that about 10 percent of collection is upstream. On the order of magnitude, I just don't know the exact number.

MS. BRAND: Okay. So you said in an earlier round of questioning that upstream, collection from upstream is retained for a shorter period of time than collection from PRISM and you

said that the reason for that distinction is that there's a potentially greater privacy concern with respect to upstream collection.

Can you elaborate on why, whether the additional privacy concerns that pertain to upstream.

MR. DE: Sure. And a lot of this is laid out in this court opinion that's now public. This is from the fall of 2011. I think because of the nature of abouts collections, which we have discussed, there is potentially a greater likelihood of implicating incidental U.S. person communication or inadvertently collecting wholly domestic communications that therefore must need to be purged.

And for a variety of circumstances the court evaluated the minimization procedures we had in place and as a consequence of that evaluation the government put forth a shorter retention period to be sure that the court could reach comfort with the compliance of those procedures with the Fourth Amendment. And so two years was

one element of the revised procedures that are now public.

MS. BRAND: So from what you just said that if using a legitimately tasked about term a wholly domestic communication is collected, it has to be purged?

MR. DE: If one recognizes it, yes. In fact, there's a --

MS. BRAND: Even if it has foreign intelligence information?

MR. DE: There are specifics. Off the top of my head I can't articulate all the particular exceptions in the minimization procedures but there are an elaborate set of detailed procedures that are now public that discuss how upstream collection must be treated in order to account for this concern.

And it has things like data must be segregated in certain ways where the risk of collecting a wholly domestic communication is higher, there's a shorter retention period.

Wholly domestic communications are not

permitted under the statute, and so therefore as a default rule, yes, it must be purged.

MS. BRAND: Jim, was there something you wanted to add?

Okay. I want to use the word incidental collection there again, and your definition earlier seemed to be that by incidental you mean, by incidental U.S. person collection you mean that the person on the other end of the phone from the non-U.S. person abroad is a U.S. person. That's your definition, right?

Is there another definition that you're aware of? Because you seem to be -- okay.

I think there's been some frustration with the use the term incidental in that context because it's not accidental, it's intentional. It's actually unavoidable. And so I just wanted to make sure that we're all on the same page, that by incidental you mean not accidental, not unintentional, but this is actually what we're doing.

MR. LITT: It is incidental to the

collection on the target. It is not accidental, it is not inadvertent. Incidental is the appropriate term for it.

MS. BRAND: Okay.

MR. DE: And I'd say that term I think has been used far beyond this program and historically, so there's no judgement intended. That is just a term.

MS. BRAND: Okay, okay. I'll hold the other questions for another round.

MS. COLLINS COOK: Just following up on David's question, I think it goes to a broader point which is that there is a perception that this statute is fairly complicated, there's got to be loopholes or idiosyncrasies in there somewhere.

But let me just ask you, would it be the view of the United States government that it is appropriate to use 702 to intentionally target U.S. persons, whether directly or through reverse targeting, whether they are inside the United States or outside the United States?

MR. LITT: No, definitely not.

MR. DE: No.

MR. LITT: That is not permissible.

MS. COLLINS COOK: I wanted to also follow up on a question about the abouts. And I apologize, again just for folks understanding that we spent six and a half hours talking with folks about just the oversight mechanisms in place and were unable to get through that entire conversation. So I apologize if you've said this before today.

The collection methods, procedures that you use with respect to abouts, those procedures, are they approved by the FISA court?

MR. DE: Yes.

MS. COLLINS COOK: Are those transparent to Congress?

MR. DE: Yes.

MS. COLLINS COOK: I think we haven't necessarily, we started to allude to this but can you talk a little bit about your impression of how the intel committees in particular view their obligations with respect to oversight of your

programs and whether you have found in your experience that to be pro forma or in any way lacking?

And let the record reflect a few, not quite eye rolls, but I think the response was, no, they have not found this to be pro forma in any way.

MR. LITT: I've been on this job now for getting on towards five years and I have found nothing about my interactions or our institutional interactions with the intelligence committees to be pro forma.

They have fairly substantial staffs which have a lot of experience. Some of them come from the community. They know, they dig very deeply into what we do. The DNI occasionally uses the term wire-brushing for the interactions that we have with the committees, so it's not a pro forma interaction in any way.

MR. DE: If I could add one point, on programs like 702 that we're talking about today for example, we all lived through the

reauthorization of Section 702 in 2012.

That process was not simply in connection with the intelligence committees, but I can remember numerous briefings where we would go up for a member, for all member briefings that the intelligence committees would host for the Congress.

So I don't want to leave the impression that it's only with the intelligence committees, particularly for a program like 702 that needs to be voted on by all members of Congress on the basis of a sunset clause.

MS. COLLINS COOK: I want to make sure that my colleagues have time for their last round of questions so I'll cede my time.

MR. DEMPSEY: Going back to the minimization procedures question, and specifically the incidental collection question, am I right that the rule is that whether the information is inadvertently collected, that is you were tasking on the wrong selector or some mistake was made and you got something that you didn't intend to get

that's inadvertent, or you were correctly targeting the right account and then you collected communications to or from a U.S. person that's incidental, the procedures say, minimization procedures, rules say that if you never discover that it was inadvertent and never discover that it was incidental, you never realized that it was a U.S. person collection, it's deleted after five years?

The basic rule is you keep it for five years, you keep everything for five years, two years on upstream, five years on PRISM, and then it gets deleted. That's the baseline rule, right?

MR. LITT: Correct.

MR. DEMPSEY: And then you on top of that the rule is that if then you, through analysis, through reviewing it that it was inadvertent or incidental collection on a U.S. person you must immediately purge? Bob's shaking his head.

MR. LITT: There's a difference in the way inadvertent and incidental, as you're using

those terms, are very different concepts.

Inadvertent refers to a collection that was not authorized by law. That is purged.

Incidental --

MR. DEMPSEY: Purged unless?

MR. LITT: Unless, as Raj mentioned, that there are certain exceptions. I'm certainly not able to recite them but they do exist. But they're fairly narrow.

Incidental is collection that is authorized by law. And at that point the rules relating to U.S. persons kick in and if you determine that it has no foreign intelligence value you purge it.

MR. DEMPSEY: Right, but I mean what's your response to the argument, well, fine, that just means that if you think it's valuable you can keep it, if you don't think it's valuable then you purge it?

MR. LITT: But it's lawfully collected.

MR. DEMPSEY: Fair enough. But you do, if it is of interest to you, you do keep it?

MR. LITT: If it's of potential foreign intelligence value --

MR. DEMPSEY: Minimization means --

MR. LITT: If it can be useful to providing the intelligence that policy makers need or to protecting the nation against threats, then yes, we keep it for the required period.

MR. WIEGMANN: So again, to make it more concrete, if it's a terrorist overseas, he is calling a number in the United States that belongs to a U.S. person, we want to keep that information. It is incidental, the fact that we're getting the U.S. person number and we're targeting that non-U.S. person overseas, but he's calling Minneapolis, we want to keep that communication because it's of high interest to us.

MR. DE: One point I would add is just that minimization refers to steps in the process, everything from collection to review to dissemination. And so I think we're talking about one element here, and to retention. And so there are different stages in the process.

To disseminate that information a certain threshold would have to be met and so forth.

MR. DEMPSEY: Yeah, I wish there were some way, I mean I know it's totally now embedded both in law and guideline and practice, but minimization means different things.

Minimization means keep it for five years and then delete it, minimization means don't disseminate identifying information, minimization means delete it unless it's intelligence information. Those are very different.

MR. LITT: Well, they all fall within the statutory definition of minimization essentially. I'm going to mangle it a little bit, but it's procedures that are designed to minimize the acquisition, retention, and dissemination of information about unconsenting United States persons consistent with the need to produce foreign intelligence information.

And so you're going to have different minimization rules based on the particular

missions of the agencies. You're going to have different minimization rules depending on the nature of the activity you're governing. You're going to have different minimization rules depending upon the nature of the information. But minimization is that entire category of rules.

MR. DEMPSEY: But it is a little bit of a circular definition which means different things in different contexts. Sometimes it means you've --

MR. LITT: I'm not sure I'd say circular but I would say it means different things in different contexts.

MR. WIEGMANN: It's a balance.

MR. BAKER: If I could just real quick just to emphasize, you know, as Bob was just alluding to, the FBI does have its own standard minimization procedures with respect to this type of activity. I assume you've had access to those.

So anyway, there's a lot on the table that we just talked about with respect to minimization, but I would direct you to those as

well in terms of understanding the FBI's role.

MR. MEDINE: Judge Wald.

MS. WALD: When a U.S. person information that's been, quote, incidentally acquired and kept for legitimate reasons or whatever in the base is disseminated to foreign governments, as is permitted under certain circumstances, it said that it's usually masked.

I think it would be useful for public consumption to know what the masking process entails, and in what circumstances it isn't masked, and whether or not the different agencies can use different criterias for masking or it's all centralized by Justice or the Attorney General's provision.

MR. DE: Well, I can speak just for masking generally at NSA, and abstracting from the second party issue for a moment, is substituting a generic phrase like U.S. person for the name of the U.S. person that is actually collected.

And that U.S. person is a legal term. Obviously that means an individual or it could

mean a U.S. company or firm.

I don't think there's a centralized process. That's how we do it at NSA. I think that's how other agencies do it as well.

MS. WALD: But different agencies decide how to interpret their own criteria as to what should be masked and what shouldn't?

MR. LITT: It's part of the, in the 702 context it's part of their minimization procedures.

MS. WALD: Well, so what does that tell me? No, I mean specifically as to whether or not in what circumstances it's not masked, that's up to each agency, or not?

MR. LITT: Yeah, it's done on an agency by agency basis.

MR. WIEGMANN: But generally speaking, I think the minimization rules of each agency generally would not permit you to disseminate U.S. person information where that is not either foreign intelligence or necessary to understand that foreign intelligence. So in other words --

MR. DE: Or evidence of a crime.

MR. WIEGMANN: Or evidence of a crime for FBI.

So in other words, if I need to, if it's Joe Smith and his name is necessary if I'm passing it to that foreign government and it's key that they understand that it's Joe Smith because that's relevant to understanding what the threat is, or what the information is, let's say he's a cyber, malicious cyber hacker or whatever, and it was key to know the information, then you might pass Joe Smith's name.

If it was not, if it was incidentally in the communication but was not pertinent to the information you're trying to convey, then that would be deleted. It would just say U.S. person. It would be blocked out.

So they were in communication with, and it would just say U.S. person. So that's essentially how it works I think more or less in all the agencies. Is that a fair description, Raj?

MR. DE: Yeah, the basic parameters for FISA collection are articulated in the statute, the big principles of necessary to understand foreign intelligence or evidence of a crime. And then that's effectuated through the minimization procedures that each agency has. That's for 12333 collection. It's articulated, as Bob mentioned, in 12333.

MS. WALD: With those last subpart, would those, just take NSA as an example, would those mask criteria also include foreigners, non-U.S. person's information?

I mean suppose the government of Romania asks some question which might require a Rumanian non-targeted person who's in your PRISM base, would these masking procedures, etcetera, apply there too or are they just for U.S. persons?

MR. DE: In today's rule, masking procedures are for U.S. persons because they are derivative of the constitutional requirement, the minimization procedures that need to conform with the constitutional parameters for U.S. persons.

MS. WALD: So it would be up to the agency to decide whether they thought it was right or wrong to give that information to a foreign government?

MR. DE: I think there's two points to mention. One is no information would ever be disseminated unless it had foreign intelligence value.

MS. WALD: No, I know.

MR. DE: That's the entire point of disseminating that information.

MS. WALD: But having made that decision in terms --

MR. DE: If I may continue. The second point is that I think what the President has directed the DNI to examine in the PPD is what protections could be extended to non-U.S. persons. That's the study.

MS. WALD: And that's what you're working on?

MR. DE: That's the issue we're evaluating now.

MR. BAKER: One quick comment though. If I'm not mistaken, if you look in 50 USC 1806, which is Title I of FISA but I think also applies to Section 702, it says, and I don't think it restricts it with respect to U.S. person or non-U.S. person, that no federal officer or employee can disclose, can use or disclose information at all except for a lawful purpose.

So the information could only be disclosed for a lawful purpose. And I believe that's across the board.

MS. WALD: I don't have anything more.

MS. COLLINS COOK: I wanted to make sure I understood though both Judge Wald's question and the response.

I understood her to be asking under what circumstances dissemination could be made to a foreign government.

Are there separate agreements and procedures that might govern in that instance or are analysts able to simply decide they would like to provide foreign intelligence information to

foreign governments?

MR. DE: At least our procedures, our publicly available procedures have provisions that address sharing with second party partners. I don't have at my fingertips the details, but I can certainly get back to you on that. But they are now public and articulate the circumstances under which information can be shared with second party partners. Those procedures are approved by the FISC annually.

MR. LITT: I think that the critical point is that these are part of the minimization procedures that have to be approved by the FISA court to the extent we're talking again about Section 702.

MS. WALD: The minimization procedures are only for U.S. persons, aren't they?

MR. LITT: Yes, that's right.

MS. WALD: But I was talking --

MR. LITT: But there are general rules about when we can share FISA information.

MR. MEDINE: All right. Well, I want

to thank the panel very much for spending a fair amount of time with us today and discussing these issues in a public setting and we appreciate it.

And we'll take a short break and then we'll resume at eleven o'clock with our second panel. Thank you.

(Off the record)

MR. MEDINE: We're now ready to begin our second panel, and we are very pleased to be joined by Laura Donohue, who's a Professor of Law at Georgetown University Law School, Jameel Jaffer, for a return engagement, Deputy Legal Director at the ACLU, Julian Ku, who's a Professor of Law at Hofstra University, and Rachel Levinson-Waldman, who is Counsel for Liberty and National Security Program at the Brennan Center for Justice, and each will make a brief set of remarks, if you want to start.

MS. DONOHUE: Sure. Thank you very much for the opportunity to be here today. I'm looking forward to the discussion on 702.

I'd like to confine my remarks to four

central areas, just my initial remarks, and raise statutory and constitutional concerns.

First is with regard to targeting. I'm particularly concerned about four areas here. First is the inclusion of information about targets, and not just to or from targets.

Second is the burden of proof regarding whether somebody is a U.S. person or not.

Third is with regard to the burden of proof regarding the location of the individual. That is, if the NSA in either instance does not confirm, does not actually know where they are, the assumption that is built into the minimization and targeting is that it is neither a U.S. person, nor are they domestically located. And there is no affirmative duty for due diligence on the NSA to actually check their databases to find out if that individual is or is not a U.S. person and is or is not in the United States. And then the implications for the right to privacy.

In the second area on the post-targeting analysis, I'm particularly concerned

about the role of FISC, that it's severely circumscribed and that we're having warrantless searches.

So in the last panel we heard about that moment at which the information is obtained is not a search because it's foreign intelligence and there's an exception for the gathering of the intelligence.

But when information is then used for criminal prosecution, then at that point when the data is searched, if it were a case where if I were, say, speaking with a mobster in the United States and they happened to overhear incidental to my communications that I was engaged in other criminal activity, they would have to go to a court to obtain a warrant to then put a wiretap on my phone and listen to the content of my communications.

In this situation they don't do that and then they find that individuals are implicated in criminal activity and refer it for criminal prosecution.

And I would be happy to address the 2002 Foreign Intelligence Surveillance Court of review opinion that addressed this aspect, but it was with regard to Title I where there was probable cause that had already been established that the target in that case was a foreign power, an agent of a foreign power.

In this particular case, the individual is not themselves the target of any investigation and so the prerequisite Fourth Amendment threshold has not been met.

The third area is the retention and the --

MS. COLLINS COOK: Can you slow down just a bit? I can't keep up. Thank you.

MR. MEDINE: And we also have a court reporter who's probably her fingers are slowing down.

MS. DONOHUE: Sorry, I beg your pardon. I realize we only have a few minutes, and I also have written remarks which I'll be submitting.

MS. COLLINS COOK: I have reviewed

them. Thank you. I've reviewed what you've submitted thus far.

MS. DONOHUE: Right. So I will be submitting on these particular points following the hearing.

On the third area, the retention and the dissemination of data, and this came up with Judge Wald's question on the previous panel, there are a number of exceptions in terms of when the information itself has to be expunged.

The foreign intelligence information exception I would direct your attention to. It's not defined in either Section 702 specifically, or in the minimization or targeting procedures.

It is, however, defined in FISA to include any information that would be helpful for foreign affairs, which would include economic information, it would include political information, it would include a whole range of data.

The retention, dissemination for criminal prosecution, I've raised the Fourth

Amendment concerns. We're starting to see now in courts what's called parallel construction where individuals where information has come from intelligence agencies' programs, is then passed on to law enforcement, who then must create a parallel trail for probable cause, but the actual tip or initial indication of criminal activity came from intelligence.

And it essentially covers the traces that this initially arose within FISA or within Section 702, and I have increasing concerns, certainly as a scholarly matter, about the growth of parallel construction.

The client attorney privilege you had already mentioned in the last panel. That continues to be, I think, an area of some concern, not just because it's, not just in the post-indictment stage but in terms of all communications with attorneys prior to and in the context of the interception of content.

The retention of encrypted communications was not mentioned in the last

panel. All encrypted communications are retained according to NSA documents, as well as the technical barriers. If there are technical barriers they also will simply keep the information.

The other aspects of this have to do with multiple databases and CIA access, which I was surprised you didn't have the General Counsel of the CIA on the last panel. We now understand from NSA documents that the CIA has a separate set of minimization procedures and also uses Section 702. And I think that's important to take a look at what those procedures are, both the targeting and the minimization.

Finally, the fourth area that I'd just like to raise is the First Amendment concerns that I have. As has been well-recognized in the judicial system, First and Fourth Amendments often travel hand in hand, especially in national security when political matters are on the line.

And in this particular instance not only do we have a general First Amendment concern

but we know that if individuals visit IP addresses, for instance, that have been associated with particular targets, then their correspondence, communication, emails, etcetera, and other information is also retained.

What if that IP address is Al Jazeera, let's say? What if that IP address happens to be a media or a news site that's been associated with a particular area of concern? Then I think there are also First Amendment implications that follow from that.

So in conclusion I'd be happy to talk in more detail about each of these areas, the targeting, the post-targeting analysis, the retention and dissemination of data, and the final First Amendment concerns.

MR. MEDINE: Thank you very much. Mr. Jaffer.

MS. DONOHUE: Thanks.

MR. JAFFER: Thanks for the opportunity to appear before the Board.

The ACLU's view, as you already know,

is that Section 702 is unconstitutional. The statute violates the Fourth Amendment because it permits the government to conduct large scale, warrantless surveillance of Americans' international communications, communications in which Americans have a reasonable expectation of privacy.

In our view, the statute would be unconstitutional even if the warrant requirement didn't apply because the surveillance it authorizes is unreasonable.

As I discuss in more length in my written testimony, the statute lacks any of the indicia of reasonableness that the courts have looked to in upholding other surveillance statutes, including Title III and FISA.

But the point that I would like to emphasize today is that even leaving the constitutionality of the statute to the side, the government is claiming and exercising more authority than the statute actually gives it.

I say that for three reasons. First,

while the statute was intended to augment the government's authority to acquire international communications, the NSA's minimization and targeting procedures give the government broad authority to acquire purely domestic communications as well.

That's because the NSA's procedures allow the agency to presume that its targets are foreign, absent specific evidence to the contrary, and because the procedures don't require the government to destroy purely domestic communications obtained inadvertently.

Instead, they permit the agency to retain those communications when they're believed to contain foreign intelligence information, a phrase that is defined very broadly.

Second, while the statute was intended to give the government authority to acquire communications to and from the government's targets, the NSA's procedures also permit the government to obtain communications that are merely about those targets.

And that practice, in my view, finds no support in the language of the statute or in the statute's legislative history. But it's a practice that has profound implications for individual privacy.

In order to identify the communications that are about its targets, the government has to inspect every communication. To endorse the practice of about surveillance is to say that the government can surveil literally everyone, or at the very least that it can surveil every communication in and out of the country.

Finally, while Section 702 prohibits reverse targeting, the NSA's procedures authorize the government to conduct so-called back door searches, searches of communications already acquired under the FAA using selectors associated with particular known Americans.

Given the absence of any meaningful limitation on the NSA's authority to acquire international communications under Section 702, it's likely that the NSA's databases already

include the communications of millions of Americans.

The NSA's procedures allow the NSA to search through those communications and to conduct the kind of targeted investigations that in other contexts would be permitted only after a judicial finding of probable cause.

And if I have thirty more seconds I would like to make just one final point. Today we're focused on Section 702, but it's important to understand that Section 702 is merely one expression of a broader philosophy.

Yesterday the Washington Post reported that the NSA has built a surveillance system called MYSTIC capable of recording all of a country's phone calls, allowing the NSA to rewind and review conversations as long as a month after they take place.

MYSTIC is the logical endpoint of the arguments that the government is making here today. So the stakes and the conversation that we're having today are very high. It's very

difficult to believe that democratic freedom would survive for long in a system in which the government has a permanent record of every citizen's associations, movements, and communications. Thank you.

MR. MEDINE: Thank you. Professor Ku.

MR. KU: Thank you, and thanks also for the opportunity to appear before the Board today.

I just want to remind -- I have a different view I think from most of the panelists, and I apologize for not getting my remarks ahead of time.

I just want to remind the Board of two under-emphasized points of constitutional law that I think should frame our understanding of the U.S. government's surveillance practices under Section 702.

I mean first, it is important to remember that Section 702 and FISA itself need to be interpreted and understood against the history, and tradition, and the background of the President's broad, inherent executive power under

the Constitution to conduct electronic surveillance of foreign governments and foreign agents, especially overseas.

Second, although we often speak loosely of the Fourth Amendment's limitations on this presidential foreign surveillance power, it's worth noting that courts have repeatedly upheld wide-ranging, warrantless U.S. government surveillance overseas, even of U.S. citizens.

So these two constitutional observations should frame any legal assessment of Section 702 and FISA in general.

If you keep in mind the background and where we're coming from rather than where we are, 702 is not an ineffectual attempt to regulate lawless executive conduct, as the critics would have it.

In actuality, Section 702 almost certainly requires more limitations than are actually required by the Constitution and may even, although I'm not taking that position, but could in some circumstances encroach on the

President's foreign affairs powers to conduct foreign intelligence activities.

So let me just briefly elaborate on these two claims about constitutional law, which I'm sure some folks might disagree with, but this is not a dispute that U.S. presidents have long exercised the power under the Constitution to conduct foreign intelligence, and this uncontroversially flows from the President's role as the chief of foreign affairs under the Constitution. And almost every court considering the question has concluded that the President, has agreed that the President possesses an inherent constitutional authority to conduct foreign surveillance. And this is undisputed by any court.

In other words, there does not need to be statutory authorization for the President to engage in foreign surveillance.

Prior to the enactment of FISA in 1978, the executive branch claimed, and the courts did not dispute that it possessed a broad

constitutional power to conduct surveillance for foreign intelligence purposes, even inside the United States and usually without a warrant.

So prior to the enactment of Section 702 and its predecessors, the executive branch claimed a constitutional power to conduct warrantless surveillance in foreign countries for foreign intelligence purposes, whether or not that surveillance included a U.S. citizen who was physically overseas.

So given this history I'd ask the Board to keep in mind that Section 702 and its predecessors placed more constraints on the executive branch's conduct of overseas foreign intelligence gathering than has ever been imposed in prior, in the past.

You might conclude that we need even more constraints, but we should not kid ourselves that existing constraints or even more constraints as proposed by some other folks, are consistent with historical practice and tradition and moves us further toward constraints.

As to my second point, I do not believe the Fourth Amendment imposes limitations on foreign intelligence as strict as those employed, imposed by Section 702. And let me just briefly explain the two reasons why.

First, it is very clear the Fourth Amendment does not apply to non-U.S. citizens and when they are outside the territory of the United States. And the Supreme Court confirmed this in the 1990 decision of The United State versus Verdugo-Urquidez.

So foreign citizens or the surveillance of foreign citizens outside of the United States is completely unconstrained by the Fourth Amendment.

Second, the courts have confirmed that it's highly unlikely the Fourth Amendment's warrant requirement applies to surveillance of U.S. citizens when they're outside of the United States, especially when the surveillance is conducted for foreign intelligence purposes.

No court in the United States has held

that a warrant is required for a search of a U.S. citizen when they are overseas if that search was conducted for foreign intelligence purposes.

Some courts like the second circuit have even held that no warrant is ever required for an overseas search, while others have relied on a broader foreign intelligence exception.

So there is further details here about the reasonableness, and courts have generally interpreted the Fourth Amendment's reasonableness requirement very generously in favor of the government when conducting overseas searches.

Again, in light of this long history and tradition of the United States conducting essentially unsupervised foreign intelligence gathering without any statutory authority, this is actually the tradition in the U.S. system prior to the enactment of FISA, then more recently Section 702.

So just to conclude, if you look at Section 702, the government faces a complete ban on the intentional targeting of any United States

person reasonably believed to be outside of the United States. And there are other procedural mechanisms, as you know about.

But I don't believe that actually the Fourth Amendment would actually require if there was no Section 702, the Fourth Amendment would require that the government could not intentionally target a U.S. citizen overseas and their communications.

So let me just conclude, I believe Section 702 should be understood as a sensible compromise between privacy interests and the continuing need to conduct aggressive foreign intelligence gathering. Congress has given its blessing to broad-based overseas surveillance that was already occurring pursuant to the President's inherent constitutional power.

Congress has now imposed limitations on those activities that go beyond what I believe the Fourth Amendment requires, but I think that's a small price to pay, and many of us agree, to minimize privacy intrusions into Americans'

overseas communications. And the courts are involved to provide oversight.

This is the type of political compromise and cooperation between different parties and different branches of government that we always wish, we always say we want, and so I think we should applaud it rather than condemn it.

MR. MEDINE: Thank you.

Ms. Levinson-Waldman.

MS. LEVINSON-WALDMAN: Thank you, of course, for having me here. I have a few brief comments and then I hope we'll also have a chance at some point potentially to respond to comments that were made during the first panel or during this panel.

So I'm just going to focus briefly on two primary issues that are reflected in my written submission for now.

First, I know of course that the Board is particularly interested in whether this about collection complies with the letter or spirit of Section 702. And based on the structure of the

statute, we believe that it doesn't.

Briefly, there are two main restrictions reflected in Section 702 on the collection of communications. So that would be the first, the acquisition cannot target U.S. persons or persons known to be within the United States. This is a geographic or nationality and residence restriction.

And second, that the purpose of the acquisition must be to acquire foreign intelligence information. And that's basically a content restriction. What that means is that the content of the communications that can be picked up by electronic surveillance is regulated by the foreign intelligence restriction, while the class of people who are subject to electronic surveillance is regulated by the targeting restrictions.

When communications that are about a target are collected, we believe sort of the what and the who of the collection are conflated, and that that's contrary to the clear structure of the

statute.

And we know that the results of the collection, our intention with the foreign intelligence requirement of the statute, that is, if communications that merely mention certain targets are collected then we know that significant quantities of communications that contain no foreign intelligence information whatsoever are acquired, which would appear to undermine the significant purpose requirement in the statute.

And of course this has been confirmed in the 2011 FISC opinion that was referred to that's been declassified. We learn in fact that the NSA does acquire tens of thousands of wholly domestic communication in the course of conducting that about collection.

And so for those reasons we do think that the about collection is contrary to the meaning and the structure of the statute.

And second, let me briefly mention one of the main contributions I think the Board can

make as part of its review, and I think that some of these questions came out in the first panel, which is to shed more light on some of the ways that Section 702 is being used.

It appears that what we don't know about Section 702, certainly for the public, still outweighs or outnumbers what we do know.

Obviously there will always be things that will be properly classified and kept secret, but it seems that there are many unanswered questions that the Board is in a position to help answer, help shed some light on.

So those questions would include certainly questions about how targets, and selectors, and key words are used. Some of those were answered in the first panel, but I think some of those answers also raised more questions.

There has been the suggestion, the strong suggestion from the 2011 minimization procedures that all encrypted communications can be retained by virtue of their being encrypted, and finding out if that, in fact, is true. And if

not, if the PCLOB can obtain and provide additional information about that provision.

And finally, and this is something that Laura mentioned as well, that domestic communications can be shared with law enforcement agencies if they are reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed.

In addition to raising, I think, a host of constitutional issues at the very least, and practical issues, one of the things that we don't know is whether there are minimum standards for how severe, for instance, such a crime has to be in order to share this information, which of course has been collected without a warrant.

So I hope that the answers to some of these questions also will come out during this process. Again, thank you for the opportunity to address the Board.

MR. MEDINE: Great, thank you very much for your opening statements. I'm going to ask you some questions but any panelist should feel free,

I may ask them to a specific person but anyone should feel free to jump in.

Professor Ku, you talked about the limited applicability of the Fourth Amendment to overseas collections, and maybe, and suggesting there's certainly no warrant requirement and a very generous reasonableness standard.

One question I have is the collections that we're talking about under 702 technically are happening in the United States. That is, the electronic communications provider is in the United States while admittedly the target is outside of the United States. Is that a distinction that you think has any constitutional significance?

MR. KU: That's a great question. I mean I think it reflects the difficulty of this, which is the technology is changing our, the way the Fourth Amendment was interpreted in some of these older cases, right.

So in the classic Fourth Amendment overseas case it was the guy searching through the

house or the apartment physically overseas of the U.S. citizen, or of the phone call that occurred on the foreign networks, right, in the foreign country.

Here we have this kind of weird situation where you have phone or communications sort of transiting through the United States. And I do agree that that might raise a harder Fourth Amendment issue, but I do think that the larger thing to keep in mind is that the geography matters because if there's a foreign person on the other side of the line, so to speak, that's I think in part the way the communication is an international communication. It has different implications for that perspective.

But I do agree that the Fourth Amendment, the territorial aspect of the Fourth Amendment would be less significant in that context.

I think the broader point though is that the courts have been very generous, both domestically and internationally about

surveillance conducted for foreign intelligence purposes.

So even, so the territorial distinction was something that FISA created, because prior to that I think FISA, the foreign intelligence gathering occurred both domestically and internationally, and the fact that it was for foreign intelligence was what mattered.

FISA has created this sort of territorial division, which I think is becoming less important with the changes in the types of communication we have.

MS. DONOHUE: If I may add to that. You know, Professor Ku brings up the exception for foreign intelligence gathering for purposes of surveillance. That's very different from the acquisition of information for purposes of prosecution. And here courts have very clearly ruled that even in cases of national security or domestic security, a warrant is required.

This is U.S. vs. U.S. District Court, a case handed down in 1972 in which there were three

individuals conspiring to bomb the CIA. And the court said that the executive branch, quoting Justice Brownell (phonetic) and others said the court -- the executive branch is not a disinterested neutral observer and cannot be put in the position of having to determine whether a search will be reasonable. They have to seek a third opinion on that.

In Katz as well in 1967, some of the justices in that case, Justice Byron White said, went beyond the decision and said basically we should not require a warrant procedure for the magistrate's judgement if the President of the United States, or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable.

And other justices responded very angrily to that statement. Justice William Brennan, Justice William O. Douglas, they pointed out that there was a conflict of interest here. They said, look, neither the President nor the

Attorney General is a magistrate. In matters where they believe national security may be involved they are not detached, disinterested, and neutral as a court where the magistrate must be.

The Foreign Intelligence Surveillance Court of Review has also considered whether or not information obtained from FISA warrants could be used in the event of a prosecution.

In the case that brought down the wall in 2002, the court looked to Title I of FISA where probable cause had been established that an individual was a target, sorry, that the target was a foreign power or an agent of a foreign power and said in that case you have this review that has gone on specific to that target by the Foreign Intelligence Surveillance Court.

In Section 702, individuals who may be brought up on criminal charges are not themselves the target of any investigation. No probable cause has been established for their involvement as a foreign power or an agent of a foreign power.

Instead, once the content of

conversations are obtained, then the government may go through, analyze the information and look for evidence of criminal activity, which can then bring them into a courtroom to face criminal charges, and at no point is this warrant requirement, which the court has held for domestic security cases. So here you have a U.S. person on U.S. soil and the court has said in U.S. vs. U.S. District Court, you have to have a warrant in that situation.

So to use the veneer of, well, we're just collecting foreign intelligence and the executive branch has the right to do this under Article II, yes, perhaps the executive branch can gather intelligence but if there are criminal penalties associated then you also need to meet the requirements of the Fourth Amendment for U.S. persons.

MR. MEDINE: I'd like to give Professor Ku a chance to respond, although I can do it on my next round.

MR. KU: Okay. Well, I mean I'm not

going to go through all the cases. And I think that the way I understand this is the way you think about this is the foreign intelligence purpose, right. The foreign intelligence purpose has been sort of an important part about whether there's an exception to the warrant requirement, or if there's a foreign intelligence purpose, sometimes a primary purpose, or a purpose, depending on how you define it. And then there's the, whether that gives a question of reasonableness, where there's legitimate government interests that goes to the reasonableness.

The reason I'm emphasizing the significance of the foreign intelligence purpose aspect of this and the territorial aspect of this is because I do think it's relevant to analysis.

This is, in fact, what's going on here is a collision between our law enforcement and intelligence goals here, right. So the U.S. government is gathering a lot of information for foreign intelligence purposes. It's also using

sometimes that information.

Some of that information is, although not I think so far frequently, leaking into criminal prosecutions. But if we start from the perspective of foreign intelligence gathering, right, this is Article II, this is where we start, and this is something that's largely been unregulated.

What's changed is that the nature of communications have changed so that many of the communications that were essentially gathered unsupervised for foreign intelligence purposes are being sort of routed in a different way so that it falls within, technically speaking, what we might consider a different sort of format, which then looks more like a classic Fourth Amendment case.

But I think that the larger point I'm trying to emphasize here is that this is, there are real Fourth Amendment issues here with respect to law enforcement.

But this is also about foreign intelligence gathering. It's not just a total

sham. It's not as if the government is claiming here that this whole thing is a scheme in order just to gather information for criminal prosecution.

Essentially they're both interests here that are part of this analysis. And that legal analysis with respect to foreign intelligence gathering needs to be considered and it should frame our analysis of what's going on here as well.

MS. BRAND: Thank you. So it's a good segue actually what you said, Professor Ku, because I want to understand, Professor Donohue, what you were saying, and I may not have taken the best notes, so forgive me.

But walk me through the argument, because a second ago you said that you were making a distinction between collection for foreign intelligence purposes and I think you said collection that was focused, was for the purpose of prosecution.

So are you, is it your view that 702

collection is for the purpose of prosecution?

MS. DONOHUE: It's one of the two stated purposes for which the information can be retained once it is collected. So it can be --

MS. BRAND: But that's different. But I'm asking about you said collected for the purpose of prosecution, I thought. I mean what is, I guess what I'm trying to get at is, is this distinction between foreign intelligence purpose and criminal purpose relevant at the collection stage only, or at all stages, or what? Help me understand what you're talking about.

MS. DONOHUE: Yeah, so in the previous panel Brad addressed this point. He mentioned that in the context of it's the moment at which the information's obtained that a search occurs, right.

So if we do our Fourth Amendment analysis at that point, then the moment at which you're obtaining the wiretap evidence is the search, at which point you would require a warrant under these.

And I believe Professor Ku's point is, no, you don't need a warrant if it's for foreign intelligence purposes at the moment you acquire the information with the international nexus to it. And he's citing Verdugo-Urquidez where there was no nexus to the United States and a search occurred overseas.

The problem is in the case, and this gets back to my first point, which I apologize if I spoke too quickly at the beginning of the panel, which is with regard to the targeting. If it is not just information to or from the target, or held by the target, but any information about or relating to the target.

And here, it's interesting, I was a little bit confused by the earlier panel because according to the actual documents the NSA has released, the NSA can actually use computer selection terms and other information such as words, or phrases, or discriminators to scan content.

So if it can collect all of the

international communications and then scan the content of those communications, then I would argue that is a search for purposes of the Fourth Amendment at the point of collection.

MS. BRAND: But let me get to this distinction though between foreign intelligence and a criminal purpose, because 702 requires not only that the collection be a non-U.S. person abroad but also that there be a foreign intelligence purpose, that the information be reasonably believed to be, to collect foreign intelligence. I'm not quoting the statute.

But doesn't that statutory requirement suggest that it has to be for a foreign intelligence purpose? And it might also then collect evidence of a crime, which then there are procedures for what to do with that information.

But it seems like you're suggesting that you think that the collection itself is for a criminal purpose, and that's what sort of piqued my interest and I wanted to understand what you were saying there.

MS. DONOHUE: Sure. So to push on this a little bit, under FISA to be a foreign power one is not a U.S. person, right, one is a foreign power or an agent of a foreign power. Not all of the agents of a foreign power require criminal showings, but many of them do.

So to say that this is purely a foreign intelligence purpose when an individual can be targeted based on being either a foreign power or an agent of a foreign power, in which case there is criminal activity involved and there may be the element of criminality from the outset. So it's not as though criminality is not an aspect of the foreign intelligence gathering generally.

MS. BRAND: Professor Ku, do you have -- Jameel, it looks like you wanted to respond.

MR. JAFFER: Well, I was just going to speak to the foreign intelligence exception more generally, if you want to pursue this.

MS. BRAND: Go ahead. Go ahead.

MR. JAFFER: Well, so I just want to caution the Board about starting from the premise

that there is in fact a foreign intelligence exception to the warrant requirement. The cases in which courts have held that there is such an exception predate FISA. There's arguably one exception to that, but the vast majority of them predate FISA.

And so their rationale has been undermined by practice under FISA over the last thirty-five years. The rationale for those cases was in large part that the courts might not be capable of overseeing collection or surveillance for foreign intelligence purposes. But the courts have been doing precisely that now since 1978.

But even if you accept that there is in fact a foreign intelligence exception to the warrant requirement, you have to ask the question of how broad that exception is.

And all of those cases, those pre-FISA cases, involve cases involved situations in which there was probable cause to believe that the target was a foreign agent, the surveillance was approved personally by the President or the

Attorney General, and the primary purpose of the surveillance was to gather foreign intelligence information.

And Section 702 doesn't include any of those requirements. So no court has ever approved a foreign intelligence exception to the warrant requirement that is broad enough to read Section 702. Section 702 is a broader statute than any foreign intelligence exception recognized so far would allow.

I think that it may also be important to emphasize that concluding that the warrant requirement applies doesn't mean that the government has to get a warrant before surveilling legitimate foreign targets. It doesn't mean that in order to surveil, you know, some suspected terrorist outside the United States the government necessarily needs to get a warrant.

But at the very least it means that the government needs to take reasonable measures to avoid acquiring Americans' communications without warrants.

It means it has to not acquire them in the first place where it cannot acquire them.

When it does acquire them, it has to destroy the communications that it acquires relating to U.S. persons.

And when in narrow exceptions it retains those communications, there should be a back-end warrant requirement so the government doesn't access Americans' communications without a warrant. That's what compliance with the warrant clause would mean.

MR. MEDINE: Ms. Cook.

MS. COLLINS COOK: So thank you all for coming. I find these panels to be incredibly helpful and informative.

Ms. Donohue, I would like to -- Professor Donohue, I apologize, I'd like to follow-up on something you mentioned at the very end of your opening remarks, and that's your position that 702 raises First Amendment concerns.

I think it's clear from my previous separate statement on our 215 report that I don't

necessarily approach the First Amendment analysis the same way, but what I would find helpful from you is if you could just describe your approach to when the First Amendment would be implicated, when concerns arise, and when something would be unconstitutional based on First Amendment concerns.

So for example, would a traditional wiretap raise First Amendment concerns, and would it potentially be unconstitutional under First Amendment concerns?

Would a traditional grand jury subpoena for bank records or credit card statements that could reveal payments to lawyers or payments to various charities or associations, would that raise First Amendment concerns? Would it be unconstitutional under the First Amendment?

So if you could just walk me through on the spectrum where you're finding concerns and where you're finding violations.

MS. DONOHUE: Sure. And just to return back to Ms. Brand's point, I agree with Jameel on

the analysis about what point it would kick in for a warrant requirement is the point at which it's either about the information, because I feel like I didn't quite answer what you were asking me and I want to make sure that I do, I answer it.

It's the point at which you're getting information about that particular individual, which is a different target, and then you analyze that information, then at that point I would believe that the Fourth Amendment warrant requirement would apply.

Okay, so in response to the First Amendment question, so the courts have recognized that there is a close link between the First and the Fourth Amendment. And I frequently find whether it's in remote biometric identification systems in view of public space and facial identification, you know, that there is a First Amendment context there as well. So it tends to be in the shadows in the room.

In this particular context, the way that I see it present is with regard to the target

that is in the statute. It's very clear that the target cannot be selected --

MS. COLLINS COOK: I'm sorry, can you actually answer the question that I had posed, which was, for example, starting with a traditional --

MS. DONOHUE: Oh, yeah, so I do not see a traditional wiretap as implicating First Amendment. I do not see --

MS. COLLINS COOK: Why?

MS. DONOHUE: Because --

MS. COLLINS COOK: Even though it could, for example, reveal the fact that I belong to the ACLU, or I have called my attorney, or I'm discussing, you know, private contents and communications. So why not?

MS. DONOHUE: Because there's a balancing that occurs with regard to the element, in this case of probable cause that you have committed, are committing, or are about to commit a crime under Title III, in which case having gone before a neutral, disinterested magistrate, a law

enforcement officer says, oh, no, I suspect that Professor Donohue is engaged in this bad activity. And I think that that balancing test basically takes that situation out of a First Amendment context.

MS. COLLINS COOK: So let's take a grand jury, and then a pen register trap and trace. So a pen register trap trace, there's definitely no determination, no probable cause. So does a traditional pen register trap trace, which would reveal potential phone calls to the ACLU, to my lawyer, very private, the existence of potentially private conversations, does that violate the First Amendment?

MS. DONOHUE: Again, with prior judicial approval and review, no.

MS. COLLINS COOK: Okay. So let's take a grand jury subpoena which can be issued by a prosecutor. So in the absence of beforehand judicial review, does that violate the First Amendment?

MS. DONOHUE: No. I would say --

MS. COLLINS COOK: So what's the factor --

MS. DONOHUE: Well, it's the same for administrative warrants, I would say in the case of administrative warrants. Here's where the tipping point is for me with PRTT, let's take Section 215 as kind of a bulk metadata collection program, or Section, what is it, 402, right, for these bulk collections of pen register trap and trace type information.

When you have the bulk collection of information in a way that changes the political discourse in society, then I think you have a First Amendment question that arises.

MS. COLLINS COOK: Okay. So is if there is a perception that there is a change in political discourse, then you have a concern about a First Amendment? It's not necessarily prior judicial review, particularized probable cause?

I'm just struggling to understand, you know, at what point there's a First Amendment implication and at what point there's a First

Amendment violation, because to me, I think it's a bit of a sea change to look at either traditional or really these FISA authorities as violating the First Amendment. I do think that that's a fairly novel approach.

MR. JAFFER: But to be fair -- to be fair, the distinction between individualized surveillance and bulk surveillance is also a bit of a sea change. And so I think the question is whether the bulk surveillance, the fact that the government is now engaged in bulk surveillance, I mean I understand that there's some dispute over the vocabulary, but the fact that the government is engaged in bulk collection or bulk acquisition of this information makes the First Amendment relevant in a way that it perhaps wasn't relevant in the context of individualized surveillance of the kinds that you were describing.

I mean I think that your question perhaps goes more broadly to the question of incidental overhears, you know. When the government defends Section 702, one of the

government's defenses is that all of this information is, about Americans is overheard incidentally.

You know, I go into this in a little more detail in my written submission, but I don't think it's fair to call this kind of collection incidental in any conventional use of the term. The collection of Americans' information is entirely foreseeable, and in fact, it was the purpose of the statute.

If you look at the statements that administration, then Bush administration officials made to justify the statute or to advocate for the statute, they were quite forthright about the purpose of the statute. And the purpose in their view was to give the government broader authority to collect information, collect communications between people outside the United States, and people inside the United States.

And obviously there's no illegitimacy to the government's interest in collecting those communications. The question is whether there are

sufficient safeguards in place, but that's why I say that incidental is probably the wrong word.

But if the government is relying on the incidental overhear cases from the Fourth Amendment context, those cases were, involved very different contexts. Those were cases in which the surveillance was individualized. It was based on a probable cause warrant.

The scale of the surveillance of the incidental collection was much different. And the fact that there was judicial oversight at the front-end provided a kind of protection for incidentally overheard people that doesn't exist under a statute like 702.

MR. MEDINE: Let's give Jim the chance to ask some questions, then we can come around.

MS. DONOHUE: Okay.

MR. DEMPSEY: Thanks. Thanks to the witnesses.

A question for Jameel and for Rachel on the abouts. What actually is, quoting the words of the statute, what is the strongest textual

argument against about surveillance?

Because the statute says the targeting of persons, never really refers to even the collection of communications or interception, etcetera, so if you're collecting something about somebody, isn't that almost paradigmatically targeting the person? Where's the text?

MS. LEVINSON-WALDMAN: I mean I think one of the -- right, there's obviously ambiguity in the statute in part, and this is one the things that I mentioned in the written submission is that target isn't defined.

And I have to say some of the answers in the first panel, which answered some questions about target and selectors, I think also opened up new questions.

I do think the strongest statutory argument, literally looking at the language, is what the statute talks about.

So it says here, literally just looking at 1881 A, subpart A, Attorney General and Director of National Intelligence may authorize

jointly the targeting of persons reasonably believed to be outside the United States to acquire foreign intelligence information.

So as I say, you sort of see implicitly, but I think you do see implicitly these two sort of halves of the targeting requirement, the foreign intelligence requirement and this kind of nationality and geographic restriction, and that when what you're doing is collecting about communications, what you're doing is kind of adding together, you're kind of conflating, you're morphing together these different parts of the statute so that the targeting has usually been literally thinking about the facility that's being used --

MR. DEMPSEY: Excuse me. The government has determined that a person is outside the United States and that collecting information about that person will yield foreign intelligence.

MS. LEVINSON-WALDMAN: Well, but I think that may be what's suggested by the about collection, but I think the foreign intelligence

determination is a separate one, right.

The government identifies these targets or selectors which have generally been to or from. And in fact we know, especially from Judge Bates's opinion that thousands, tens of thousands of communications are collected using the about targeting, the about collection, that are wholly domestic, that have no foreign intelligence value, which I think undermines an argument that there has been some determination of foreign intelligence value there, because to some extent the results are sort of speaking for themselves.

MR. DEMPSEY: Because then you would be questioning the legitimacy of the to and froms because they only do abouts about people that they also do to and froms, so you can't say that the foreign intelligence determination of the abouts is illegitimate because then you call into question the to and from.

MS. LEVINSON-WALDMAN: Well, but I think the to and from is pretty clearly contemplated by the statute, right? You target a

person, you are trying to find communications to or from them, understanding that those will have foreign intelligence value.

MR. DEMPSEY: Let me go to Jameel. Jameel, what is the best textual argument against abouts?

MR. JAFFER: Right. Well, let me first I think agree with what I think Rachel was saying at the outset, which is that the statute I don't think explicitly forecloses about surveillance or explicitly authorizes about surveillance.

But I think a fair assessment of the statutory structure and some of the statutory text leads to the conclusion that about surveillance was not contemplated by Congress. And I'll answer your question.

MR. DEMPSEY: The text, yeah.

MR. JAFFER: So here are a few aspects of the statute that I think show that Congress was contemplating, that the target would, himself or herself, be the person whose communications were acquired.

First, a definition of electronic surveillance. It says the acquisition of the contents of any wire --

MR. DEMPSEY: This is not electronic surveillance. 702 explicitly does not cover electronic surveillance.

MR. JAFFER: Well, I think that the point I'm making is relevant nonetheless.

MR. DEMPSEY: Electronic surveillance definition is irrelevant to 702. It is not -- 702 does not regulate electronic surveillance.

MR. JAFFER: I think the point that I'm trying to make is just that the entire statutory scheme, both FISA and the FAA, contemplate that the person who is the target will be the person whose communications are actually acquired.

If you look at the definition of aggrieved person, for example, which does apply in the FAA context, aggrieved person to implicitly contemplates that the person who will be raising the claim as an aggrieved person is a person whose communications are actually acquired.

And in fact, if you conclude otherwise what you are concluding is that the target would be an aggrieved person even if his or her communications weren't acquired, which I think is a nonsensical conclusion and one that the government itself would reject.

But I think it follows from accepting that about surveillance is contemplated by the statute.

And if I could just make a sort of broader point about about surveillance, we have sort of combed through the legislative history for discussions of this kind of surveillance, and it's possible we overlooked something, but we have not found any exchange in the legislative history around the FAA that suggests that Congress was contemplating about surveillance.

To the contrary, when people discuss, when legislators discuss the kind of surveillance that would take place under the statute, they discuss surveillance of the target.

And even on the government panel this

morning one of the panelists used the example, bad guy at Google.com, you know, which again is suggesting that the surveillance that's going on is of the target himself or herself.

And in defending the statute before the Supreme Court, the Solicitor General and the Justice Department more generally characterized the statute as one that allowed the government to collect targets' communications.

So you know, I think that this is an entirely a foreign concept, foreign to the legislative history and foreign to the text of the statute.

MR. MEDINE: Thank you. Judge Wald.

MS. WALD: Let me pick up on the about thing and pose one of those terrible hypotheticals. If you had a to and from, you had a targeted, a legitimately targeted person and in the process of collecting information you got, you came across this email between, I'll be facetious a bit, the grandmother of one of them to the grandmother of somebody else saying something

along the lines of, my grandson was talking to me and he was telling me all about this wonderful service he did by plotting, I'm using an extreme, plotting to blow up a facility kind of thing, I mean how would you take care of that situation where you had it between two people who are not the to and froms? You wouldn't ignore it, would you, or would you? I mean how would you handle that if you had no abouts?

MS. DONOHUE: I'm not sure whom that's directed to.

MS. WALD: I don't care.

MR. MEDINE: Who would you like it directed to?

MS. WALD: What?

MR. MEDINE: Who are you asking?

MS. WALD: Well, the two people who've talked about what about abouts, Mr. Jaffer and Ms. Levinson-Waldman, I think.

MR. JAFFER: Well, I'm not a hundred percent sure I understand the question. The question is, you know, if you were conducting

about surveillance and you come across evidence of a terrorist plot, do you really expect them to ignore it? Then no, I don't, you know.

But that's like asking, you know, if the government breaks into a home unconstitutionally and finds evidence of a terrorist plot, do I expect them to ignore it? I don't.

But we still need to ask the question what are the proper limits on the government's surveillance authority in the first place, and I think that we need to draw those limits in a way that's consistent with the Constitution.

I'm not sure that I'm answering your question.

MS. WALD: Well, you are except that I'm puzzled, too. I'm not sure I know the answer where, as I say, you had -- maybe that's an extreme example about where they have a plot, but where there's actually some foreign intelligence information which even everybody would agree had some relevance to a legitimately targeted

individual, and it's right there, and it's picked up.

MS. LEVINSON-WALDMAN: Then I think I would echo Jameel's points to some extent and sort of elaborate to say that I do think that there are always hypotheticals, presumably for any of these programs, for Section 702, for Section 215, for other collection programs that are going on where there could be some piece of information out there that might be useful that would be collected by a program.

I think it's dangerous to build surveillance programs and to think about the constitutionality and the practicality based on hypotheticals, and especially when we know that there is significant over-collection that occurs and significant collection of Americans' communications.

I think the hypotheticals are, may need to be thought about, but I don't think that they can drive how we think about the constitutionality and the statutory implications of the collection.

MS. WALD: In other words, you or anybody over there wouldn't consider if that happened, some other means that the government might have to take that about information and go to somebody, to some authority and say can we keep this, can we use this, etcetera, etcetera?

MS. DONOHUE: So what I'm a little bit confused about, and I did hear the previous panel say, oh, well, there would be all sorts of procedural implications if we had to return to a judge on the Foreign Intelligence Surveillance Court to get approval to do further monitoring.

What I'm a little bit confused about is if that information was appropriately obtained in the first place and it indicates that other people are implicated, why they wouldn't go back for a Title I electronic search and they would have what they need for that?

MS. WALD: Well, if it's two grandmothers, they're probably not -- they're just chatting. They're probably innocent. All I'm saying is I guess the only reason I raised it is

I'm trying myself to figure out are there not some gray areas here, and wondering if you had any solutions short of about authority which you find is too broad, and completely ignoring it?

But let me not use up my whole five minutes. Thank you.

I did want to ask you about, as you know, the President's review commission said they wanted to see a warrant, an actual, go get a warrant for probable cause before you could search the data using a U.S. person indicator.

My question to you is, and we've heard some reasons why they think that's very onerous, including the fact that the President's review commission's recommendation was it had to be a probable cause warrant that the person was about to commit something, do bodily injury, or about to commit some terrorism crime.

My question to you is if you think there are legitimate, and you do, problems under the Fourth Amendment with using U.S. person indicators to surveil the PRISM data, would

anything short of a probable cause warrant such as they recommended satisfy you, i.e., I'm just throwing this out, you know, having, going back to, say, to the FISA court and having them look at it to see if it, either post or pre, before they used it, approving this so-called, you know, selector, etcetera, that was in fact a reasonable cause to believe that the person had information or didn't have information?

MR. JAFFER: I don't think that would be sufficient. I think that you need a warrant at the back-end and --

MS. WALD: But what kind of a warrant warrants --

MR. JAFFER: A warrant based on probable cause and --

MS. WALD: Probable cause of what?

MR. JAFFER: Well, so I think it could be foreign intelligence probable cause, although I hope that the panel will, that the Board will think about the scope of the definition, the definitions of foreign agent, foreign power, and

foreign intelligence information.

But I think that foreign intelligence probable cause could be sufficient for that particular process, or obviously criminal probable cause.

But I also just want to say that I don't think back-end procedures alone are enough, no matter how strong they are. And I think that, you know, I know that the Board can't talk about the Washington Post report from yesterday, but if you just take it as a kind of hypothetical, you know, if you accept that back-end procedures are enough and that we'll focus solely on the protections on searching, and dissemination, and analysis of information in the government's hands, there's nothing to prevent the government from recording every phone call, copying every email, creating a permanent record of everybody's movements, associations, and communications. And the only question we'll be asking is when can the government access it.

But the creation of that kind of

massive database will have huge implications for the way that ordinary people operate in society, both the way that they interact with one another and the way that they interact with their government.

People who believe that the government is surveilling every movement and every communication, believe justifiably that it's doing it, will act differently. They won't go to controversial websites and they won't engage in controversial communications that are necessary for any democracy.

MS. WALD: I'll save, I know my time is up. I'll wait for the next round. I have another question.

MR. MEDINE: I want to go back to that back-end searching, basically the U.S. person searches, and this really is two questions.

One is the government panel asserts that this is lawfully obtained information and therefore should be permissibly used without any further Fourth Amendment implications. And why

that's not a persuasive argument.

And then two, if it's not persuasive, what is the procedure that you envision? And again, I think it's different from Professor Donohue where you're using that U.S. person information to get more information. You're just saying let's use the information we've already collected under some other, under authority for, say, criminal purposes or foreign intelligence purposes.

So I guess it's two parts. Why isn't is already legally usable? And if it's not, what procedure would you apply to access it? And that's to any panelists.

MS. DONOHUE: So as a statutory matter I would come back to the burden of proof with regard to whether that information that's being collected on targets, they are indeed U.S. persons or non-U.S. persons and located outside the United States.

So here the statute is silent, and I share Mr. Dempsey's textual analysis of the about

question. I think the statute is silent there as well. But in regard that the statute does say where you know that somebody is a U.S. person, you know, you have Sections 703 and 704 that you have to operate under.

MR. MEDINE: Again, we're not targeting the U.S. person, we're targeting a non-U.S. person, and Congress clearly knew that at the other end of that phone call could be a U.S. person and still authorized that kind of collection without a warrant.

And the question is, why isn't that sufficient to then say, okay, this information was lawfully collected, now we can do searches based on it?

MS. DONOHUE: Because it isn't certain that the person on whom you're collecting the information really is a non-U.S. person. So the burden of proof on the NSA is to say, to establish that this individual is a non-U.S. person.

But in fact, so the assumption that all

the collection that's going on currently is of non-U.S. persons I think is an erroneous one. And it's one -- and the reason why I think it's erroneous is because the NSA is under no obligation to check and see and make sure that that individual is not a U.S. person.

To the contrary, they have in their documents they say, well, they may check these databases, they may check these other databases. There's no obligation that they do so.

Mr. De in the previous panel referred to the totality of the circumstances type tests that say they have two strikes against, four strikes for, they look at everything. There is nothing that obliges them to then go back and dig up more information to find out in that particular circumstance.

And not only that, but actually if you look at the requirements for what is required to positively identify, to conclusively determine it in the minimization procedures, the bar is actually significantly high.

It means that you know their name, you know their title, your know their address, you know their personally identifiable information in the context of activities conducted by that person that are related to that particular person. A reference to a brand name, manufacturer's name, Monroe Doctrine, etcetera, that's not sufficient.

So not only are they under no obligation to establish that but in order to establish it, it's a very high bar. So it's not clear to me that that information is lawfully collected in the first place.

MR. MEDINE: Ms. Levinson-Waldman, do you want to weigh in on that?

MS. LEVINSON-WALDMAN: I think the other thing I was going to add, if I'm understanding the question correctly about why is it not okay to do searches on information that's been lawfully collected, I think there's also an element of bootstrapping.

So that it was lawfully collected for a purpose, for a foreign intelligence purpose, and

that you're right, of course Congress knew that U.S. person information was going to be incidentally collected through that process, but then there are these minimization procedures.

And so kind of almost bypassing those procedures and allowing that body of information to be collected without meeting a fairly high bar, some kind of probable cause warrant seems like kind of going back and bootstrapping your way into that information in a way that is very different from searches of, I think, any other, almost any other body of lawfully collected information, because the standard for which it's obtained, that foreign intelligence standard and purpose is so different.

MR. JAFFER: I mean I actually think there are two kinds of bootstrapping. The first is pointing to the fact that foreigners outside the United States lack Fourth Amendment rights in order to collect huge volumes of communications to which Americans are a party.

And then the other is pointing to the

foreign intelligence purpose to gather information which is then later used in criminal prosecutions. So that's to state the problem. It's not a solution to the problem, but I think that's where the concern comes from.

MR. MEDINE: Professor Ku.

MR. KU: If I could just add, I mean I'm not sure that's bootstrapping. I think that's sort of the purpose, right. The purpose is -- it's not that they're not also collecting it for foreign intelligence purposes.

It's also true that if in the old days they came across a letter from an American person to a foreign person, it seems unlikely to me that because an American sent the letter that means they can't -- but they lawfully obtained the letter, it's unclear to me why they couldn't use that letter.

And so I'm a little, possibly it's bootstrapping, but it's, there's a long history of going after foreigners and doing foreign surveillance.

I'm not sure that -- I think the only difference I think is technology does make it easier for it to flip back into the states, but I'm not sure that fundamentally this is a really different thing.

MR. MEDINE: Thank you. Ms. Brand.

MS. BRAND: Thank you. Well, it seems like there are some fundamentally opposing world views about the Fourth Amendment on the panel, and I want to, I mean this Board is not going to move Fourth Amendment law. So I want to get to what you think the law is and what you think the law should be, because I think there might be some conflation of those two things going on here.

First of all, Professor Ku, thank you for submitting your comments this morning, your written comments. I haven't had a chance to read them yet so I just want to ask you a question to make sure I understand where you're coming from.

You talk about inherent executive authority to conduct surveillance abroad or even of non-U.S. persons abroad. In your view, does

that inherent executive power operate alongside the Fourth Amendment, or irrespective of the Fourth Amendment, or does that create an exception to the Fourth Amendment?

MR. KU: Right, no, I don't think it creates an exception to the Fourth Amendment. It operates within the constraints, whatever they might be, of the Fourth Amendment.

But I would like to point out that historically this -- I mean so just to clarify. The reason I raise this, it goes to the point that historically the U.S. government as operated without statutory authority to conduct foreign surveillance. It's been, the power was granted, was thought of as coming from the Constitution.

So the statutory scheme has not been thought of as necessary to authorize the type of intelligence gathering that's going on.

Now the Fourth Amendment does apply, but as I also emphasized, it hasn't always applied. It didn't originally was thought of to apply at all, even to U.S. citizens overseas, but

I think we understand that the courts have come around to view that it does apply to U.S. citizens overseas. But I think it still has a limited impact compared to the way it applies for purely domestic searches. So that's how I would analyze that.

MS. BRAND: And how does it apply to purely domestic searches where there's a purpose of foreign intelligence gathering?

MR. KU: Well, I think that -- well, here I think that, you know, it does. The Fourth Amendment has been interpreted in recent cases to be a much more robust protection for searches domestically, although even in some of those cases, right, a warrant has not been required or the exception to the warrant requirement has been found for foreign intelligence purposes. So it still continues to exist within the domestic sphere.

I would say that for me, at least my understanding is a lot of this has been supplanted by the FISA system. The rise of the FISA system

has to some degree made the Fourth Amendment analysis a little bit less onerous because what's been happening is that everything's been funneled through the FISA system and the challenges to the FISA system has not been sort of as robust.

I think if we hadn't had FISA maybe we'd have had more cases that would have clarified exactly what the Fourth Amendment limits on domestic foreign intelligence searches would be. I do think that it applies more strongly to domestic searches and I think it has more significance.

But I do think that ultimately the foreign intelligence exception to the warrant requirement is a reasonable one that does need to be respected. It has a long tradition in history.

In my view, really FISA is sort of on top of that to add additional privacy protections that I think Congress has judged, and probably rightly so, we need. But I'm not sure the Fourth Amendment itself standing alone would necessarily require all of the sort of procedural limitations

and minimization protections that we have.

MS. BRAND: Okay. And Jameel, can you very briefly, because I have another question for you, you do not think there is any foreign intelligence exception to the Fourth Amendment? Is that what I heard you say earlier?

MR. JAFFER: I don't think that there's any foreign intelligence exception broad enough to justify 702, and no court has --

MS. BRAND: But there is -- I mean I guess what I'm trying to get at is, do you think that the Fourth Amendment applies equally to collection for the purpose of foreign intelligence gathering as it applies to collection when the purpose is to gather evidence of a bank robbery, for example?

MR. JAFFER: I think that there are certainly narrow circumstances in which the courts have held that there is a foreign intelligence exception.

Again, those cases predate FISA, and so you know, you have to evaluate whether those cases

survived the thirty-five years of experience under FISA.

MS. BRAND: Okay. And then you referred earlier to, I think you were referring to, well, you're referring to 702 generally as large scale collection. I'm not sure if you were including both upstream or PRISM in that assessment.

But if you were here for the first panel and if you take the government's facts as they stated them to be true, what about that program strikes you as large scale? What's your justification for that description?

MR. JAFFER: Well, so two responses to that. The first is I think it's important to draw a distinction between statutory restrictions and executive restraint. So there's a question of what the statute allows and then there's a question of how the government is implementing it.

Obviously I know much less about how the government is implementing it than I do about what the statute on its face allows because I can

read the statute and I have access to only a portion of the government's documents.

But then as to, you know, whether it's large scale collection or not, I think that the problem is that everybody is using these words in different ways. The panelists this morning said that they weren't drawing a distinction between acquisition, surveillance, and collection. But their own documents do draw a distinction.

If you look at USD 18, for example, which is the Defense Department's implementation of the executive order on intelligence collection, it draws a distinction between electronic surveillance and acquisition on the one hand and collection on the other.

And collection involves the tasking of that, or tasking of communications, whereas electronic surveillance and acquisition do not.

And so, you know, we have always thought of this, putting the vocabulary to the side for a second, we've always thought of this in two stages. There is a kind of, just to -- there

is a kind of, you might call it scanning, you might call it collection, but there's a kind of large scale acquisition of data, and then there's the government tasking that data, and then there is the government's tasking that data with selectors.

So to be a little more concrete, if the government installs on a switch somewhere installs a device that either diverts all of the communications or a large portion of the communications, or scans a large portion of the communications, we would call that bulk collection.

I'm not sure that anything turns on vocabulary but we should all make sure we're talking about the same concepts.

MR. MEDINE: Ms. Cook.

MS. COLLINS COOK: Actually that was right at the top of the last piece. I think we've used, and in this conversation alone we've used scan, inspect, acquire, collect, access.

And so I guess my question is, if you

have access, so in your hypothetical you've installed something that gives you access to this stream of communications, is that a seizure or a search for the purpose of Fourth Amendment analysis in your view?

MR. JAFFER: Well, I think it would depend what you were accessing. You know, the question would be have you invaded a reasonable expectation of privacy?

But we have taken the position that, for example, the bulk accessing of telephone metadata is an invasion of a reasonable expectation of privacy, and we would certainly take the same position with respect to the bulk acquisition of telephone calls or emails.

The MYSTIC program, again, just discussing it as a kind of hypothetical, that program in my view involves the bulk collection of telephone calls, voicemail messages, and telephone calls, even if the government doesn't access more than a small proportion of them.

MS. DONOHUE: May I add something to

that just very quickly? I was a little bit confused in the earlier panel because on the one hand they were saying this is a very limited program. On the other hand they say that this SIGAD is the most used NSA SIGAD.

The slides that have been released say it draws from Microsoft, Google, Yahoo, Facebook, Paltalk, YouTube, Skype, AOL and Apple, that it gets voice over Internet protocol, email, chats, all this information, and it's hard to square that.

And what they say is the value of the program, with its limited nature --

MS. COLLINS COOK: I'm sorry, can we talk about -- I appreciate your desire to talk about the previous panel but I had a specific question out that I'm really trying to understand the panelists' view on when the Fourth Amendment is implicated and how.

And so if it's under your hypothetical if you have the acquisition of all phone calls from a country with subsequent access, at what

point would the Fourth Amendment attach?

MR. JAFFER: I would say certainly the moment you put it in your databases, by that moment the Fourth Amendment has attached.

MS. COLLINS COOK: So flipping that, if it's access to a wide swath of communications but acquisition into the government's possession or control, when would the Fourth Amendment attach?

MR. JAFFER: I'm sorry, but I've lost track of the difference between access and acquisition.

MS. COLLINS COOK: And this is part of the, I think you've used scanned, but some ability to review a stream of communications and pull, filter, something to that effect.

MR. JAFFER: Right. The scanning or the filtering would implicate the Fourth Amendment in my view.

MS. COLLINS COOK: That's helpful. I wanted to follow up on a different set of questions and just close the loop.

If the determination was made that the

acquisition of the information pursuant to 702 was lawful, it's lawfully acquired information, would you still take the position that a subsequent search, and by that I mean a query using a U.S. person identifier, would need some sort of probable cause determination, that there would be a separate Fourth Amendment analysis?

And can you explain why? I guess is this because there's a view that there's a lack of particularity of the front-end and therefore you have to have subsequent some particularized finding?

MR. JAFFER: Yes.

MS. DONOHUE: That would be my position as well.

MS. COLLINS COOK: Okay. One question for Professor Ku, if I could. We've heard that 702 is silent, I think it's fair to say on the precise question of abouts. There are some structural arguments here and some purpose arguments that you can look to, but it's silent.

In view of the evolution of our

understanding of Article II of FISA, how would you as a constitutional matter assess a silence in 702? Because Title VII is both an authorization and a restriction on Article II authority, so.

MR. KU: Right. So I think, I don't know if I have any sort of grand insights on the purely textual analysis, although I do think that the constitutional background is what can help us here with respect to, if we understand where we're coming from can help us analyze this.

If we understand that constitutionally that the U.S. government was engaged in broad searches prior to the enactment of 702 then you have to sort of think about, well, to what degree.

This is not really about authorizing, this is really about restricting, imposing restrictions on what I think the U.S. government had the authority to do prior to the enactment of the statute.

And so if you look at it from that perspective then, if it doesn't, the silence or the lack of clarity or specificity would then I

think lead me from that perspective to suggest that the President retains that power.

I would analogize this a little bit to the point that was made in the earlier FISA statute, how they excluded radio completely from the original FISA, radio communications, they just said nothing about it.

And there are a lot of people that argue that was on the assumption that most of the foreign intelligence was radio in 1973 and that the President would continue going on gathering as much radio signals intelligence as he could. And then at a certain time, no one used radio anymore.

But the point is that if you add the restriction in the statute it doesn't -- the previous or the other authority the President has to conduct the surveillance should in theory continue, and I think would likely to continue here too, assuming he had the authority prior to the enactment.

MR. MEDINE: Mr. Dempsey.

MR. DEMPSEY: A quick comment and then

a question. Going to the definition of distinctions between collect, acquire, etcetera, my comment is we really have to take yes for yes and no for no and move on. The government has said, to my mind totally clearly, they are not relying upon the USD 18 concepts in implementing 702, so I think that we just have to move on from that. That's my comment.

My question is the following, and this is for Jameel or anybody, Rachel, in terms of the querying of data otherwise lawfully acquired, what is the best case law that would limit the proposition that data lawfully acquired can be subsequently queried without limitation?

MR. JAFFER: Well, so on your comment, I think you're certainly right that the government said on the panel earlier today that they were not relying on the distinction, any distinction between acquisition and collection.

But I think that the government also acknowledged that it was engaged in about surveillance, and to engage in about surveillance,

my understanding is that there is no way to engage in about surveillance without inspecting in some sense every communication within the universe of those that you are monitoring or surveilling. There's no way to do it.

Now you can call that bulk collection or you can call it something else, but that scanning of every communication in a particular universe raises constitutional issues, and if all you're saying, Mr. Dempsey, is we should just address those constitutional issues, then I entirely agree.

MR. DEMPSEY: So now as the querying of otherwise lawfully acquired communications, and let's take, you know, if I steal your computer, I think, and then I give it to the government, the government lawfully acquired it. I may have stolen it. Or certainly in the Title III context the government lawfully acquires, or in the normal search and seizure context, or in the voluntary disclosure context, where is there case law limiting the proposition that lawfully acquired

information cannot subsequently be queried essentially without prior authorization, without meeting any threshold? What is, is there any case law limiting that?

MS. DONOHUE: So we're starting to see cases come out of border security issues where computers -- border security issues, and I'd be happy to send you the names of the cases afterwards, where computers have been lawfully seized under customs laws but then they cannot be searched for all of the information on them because of the privacy implications that are involved and lack of a sufficient nexus to the suspected criminal activity.

So those cases might be one source that you would look to in a new age of data where so much information is available.

MR. JAFFER: You know, I think it's important to ask the question the other way around as well, which is, you know, where is there case law showing that the Constitution is indifferent to the government collecting huge

volumes of communications without any individualized suspicion or particularity, and then sort of bootstrapping its way into free rein or --

MR. DEMPSEY: Again, if we're in a situation, I'm just trying to pose the situation of let us assume, just let us assume that the collection was lawful.

MR. JAFFER: I'm not suggesting for these purposes that the collection was unlawful. What I'm saying is that the collection here is different in kind from the kind of collection that the courts have been concerned with in other cases involving the use of information lawfully acquired. You know, it was important to those cases not just --

MR. DEMPSEY: So then the license plate readers, the information collected by the license plate readers is lawfully acquired and then the government can subsequently query that license plate database. I mean that's standard procedure.

MR. JAFFER: I'm not sure that it's

established with any certainty that the bulk collection, that the querying of a database of bulk collected license plate reader information doesn't raise Fourth Amendment concerns, and I think that that's still an open question.

MR. DEMPSEY: Well, I'm looking for some cases. Professor Donohue has some border cases --

MS. DONOHUE: I'd be happy to send you the border doctrine cases.

MR. DEMPSEY: That may be relevant. I would welcome any other cases limiting that proposition.

MR. MEDINE: Judge Wald.

MS. WALD: This is probably an unfair question but I'll ask it anyway. Given the fact that the grievances about 702 as it operates today have included a whole series of things, one we didn't discuss here but it's been raised in written stuff is the lack of FISA review of particularized targeting designations. I know it's allowed by the statute, but nonetheless the

capture and use of incidental U.S. information to search database, the use and retention of the U.S. information.

But my question is, if you had to focus on one or maybe two important changes that you would like to see made now in 702, what would they be? Very quickly, anybody that wants to answer it.

MS. DONOHUE: I would say limiting the information to, or from, or held by the actual target and inserting a mechanism of judicial review if information is uncovered that would lead to subsequent criminal prosecution prior to analysis of the databases that are held.

MS. WALD: Okay, great. Down the line.

MR. JAFFER: The only thing that I would add to that is destruction of inadvertently acquired communications. Communications that the government itself acknowledges should not have been acquired in the first place should be destroyed immediately.

MS. WALD: Destruction, they say

they're purging them but you mean something --

MR. JAFFER: There are broad exceptions to the --

MS. WALD: I know there are exceptions, but you mean -- okay.

Do you have any, Professor Ku?

MR. KU: Actually, I mean this may be kind of not what you're looking for, but I do think that actually I would prefer the FISA section clarify the default that I've been arguing for, that it doesn't encroach, to clarify further that it doesn't encroach on, Section 702 doesn't encroach on the President's, you know, foreign intelligence authority. That would, I think, help our interpretation of the statute.

MS. LEVINSON-WALDMAN: And I just would mention three things. One is I agree more robust involvement by the FISC.

MS. WALD: I'm sorry, more?

MS. LEVINSON-WALD: More robust involvement by the FISC in terms of review. There's some review now that is sort of a

box-checking procedure, and have that review be more --

MS. WALD: Just the way they do what they do now, but more carefully?

MS. LEVINSON-WALDMAN: Well, I'd say not even, it's not so much that I think that they're not careful with it now, it's that the statute actually limits the scope of some of the review that they do, that they sort of don't get behind the curtain.

MS. WALD: Including the targeting.

MS. LEVINSON-WALDMAN: Right. I guess the second, thinking about, so if you think about Section 702 but having the minimization procedures be a natural part of that statute.

Certainly limiting and potentially eliminating the use of information for law enforcement purposes. And obviously this is something that the NSA, that the President's review group spoke to as well and made that recommendation.

And then the third quite honestly would

be to lift the standard back up to agent of a foreign power from the foreign intelligence requirement. And the foreign intelligence purpose is so loose and that that seems to be --

MS. WALD: For targeting?

MS. LEVINSON-WALDMAN: For targeting, yes, that's correct.

MS. WALD: Okay. I've got maybe one minute left so a quick question. Some of you, I don't remember now, all of you in a prior one, when we were doing 215, talked about the desirability/necessity of having an adversarial element in the FISA proceedings.

A very quick notion of how would you see an adversary, however appointed, in a 702 proceeding? In other words, what function could they serve, he or she serve in a 702?

215 was a little bit more evident. A novel technological case coming up to the court, what would you say, do they have any, would they have any function in a 702?

MS. DONOHUE: So I would imagine them

having a function absolutely, yes. The ACLU tried to do this and was not allowed to intervene on a motion on a First Amendment grounds and it was denied by the court in part on the grounds that they would never succeed on the First Amendment to actually intervene.

I think having an advocate there would allow them to more carefully review minimization procedures, to more carefully review targeting procedures. It would allow them to evaluate the role that they play with regard to targeting.

MS. WALD: In individual cases in 702?

MS. DONOHUE: And in individual cases, yes, but you would have to change to insert some sort of a warrant requirement equivalent for criminal prosecution or further examination of the records.

MR. JAFFER: And I think that our biggest concern is with judicial rulings that have far-reaching implications and not just implications in the individual cases. So I think that when you're talking about the individual

cases, I do think that, you know, in theory an adversarial process would be a useful thing.

On the other hand, I think that the closer you get to an individualized warrant application, or court order application, or surveillance application, the more it looks like traditional Title III or a search warrant context, which is ex parte.

But you know, when you get to judicial opinions that authorize about surveillance at some level of generality, that is something that ought to be argued in open court, you know, with a closed hearing to follow if there is legitimate, if there are legitimate sources and methods to be protected.

But if I can just use the process to add one answer to your previous question, I agree very strongly with what Rachel said that reforming or revising the standard, the targeting standard is crucial.

Right now there is, there's really no limit on who the government can target overseas.

The example that the government panelist kept coming back to is bad guy at Google.com or bad guy at Yahoo.com. But it could as easily be journalist at Yahoo.com, or human rights activist at Yahoo.com. And I think it's crucial that some limits be drawn around the category of people whom the government can legitimately target.

MS. WALD: And by the FISA court?

MR. MEDINE: We only have a couple of minutes. If there's any members of the Board who want to ask any additional questions.

MS. COLLINS COOK: Can I ask just one quick follow-up question on this point actually?

MR. MEDINE: Sure.

MS. COLLINS COOK: And this is to Ms. Levinson-Waldman. You had said lift the standard back to agent of a foreign power or a foreign power. What were you referring to when you said back to?

MS. LEVINSON-WALDMAN: Right, I mean I guess back to, we're sort of envisioning to some extent Section 702 is sui generis and when it came

into being it was a foreign intelligence requirement. But I guess thinking of FISA more broadly, narrowing that foreign intelligence standard in some way to match what is in other sections.

Obviously one option would be matching what's in other sections of FISA, agent of a foreign power, I think that would be our preference, but narrowing that in some way. Back was probably an imprecise way of referring to it.

And if I could add one other brief thing, I think our other, you know, if we have a wish list it would be, and again, I'll say restore, but thinking about other parts of FISA, having the collection be, and you know, these may be one or the other but having the collection, the foreign intelligence be the primary purpose rather than a significant purpose, that that has also allowed, you know, potentially a fair amount of slippage in terms of what the collection is for.

MR. MEDINE: Any other final questions? I want to thank the panelists very much for

joining us today. It was a very enlightening discussion. We're now going to take a lunch break and we will resume with our third panel at 1:45. Thank you.

(Off the record)

MR. MEDINE: Good afternoon, and thanks everyone for rejoining us. And I want to introduce our third panel, which will be on transnational and policy issues.

We are joined by John Bellinger, who is a partner at Arnold & Porter, Dean Garfield, who is the President and CEO of the Information Technology Industry Council, Laura Pitter, who is a Senior National Security Researcher at the Human Rights Watch, Ulrich Sieber, who is the Director at the Max Planck Institute for Foreign and International Criminal Law in Freiburg, Germany, and Chris Wolf, who is a partner at Hogan Lovells.

Each of the panelists will make a brief opening statement and then we will proceed with the Board questioning.

I guess we can start alphabetically

with Mr. Bellinger.

MR. BELLINGER: It's me first then. Well, thank you all very much for having me in, the members of the Board. I'm going to focus my comments on whether international law places any restrictions on electronic surveillance of foreign nationals outside the United States.

I think you know I served as the legal advisor for the Department of State from 2005 to 2009, as the legal advisor for the National Security Council from 2001 to 2005, and then I was the national security advisor to the head of the Criminal Division at Justice Department before that, so I have extensive experience, both in intelligence activities and international law.

So in recent months I think you know many scholars and human rights advocates have argued that NSA surveillance of foreign nationals violates a so-called universal right to privacy recognized in international law.

They base their argument on Article 17 of a human rights treaty called the International

Covenant on Civil and Political Rights, which the U.S. ratified in 1992.

Article 17 provides, and I quote, no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence, end quote.

The argument that NSA surveillance violates Article 17 of the ICCPR is incorrect for several reasons. And I will say in my view international law, neither the ICCPR or any other part of international law placed international legal restrictions on the NSA, any of the NSA programs.

With respect to the ICCPR, first, for the last sixty-four years the United States government has taken the consistent position that it does not apply outside the borders of the United States. The U.S. took this position when we negotiated the treaty in 1950, and we re-articulated it in 1995, when the Clinton administration submitted its first report to the U.N. Human Rights Committee, which is the group

that oversees compliance with the ICCPR.

My predecessor at the time, the then legal advisor Conrad Harper, explained to the committee that the ICCPR imposes obligations on the United States only inside the United States. And that's because Article 2 of the ICCPR, which defines its scope, says that a state party is bound to respect and ensure the rights in the ICCPR only to all individuals within its territory and subject to its jurisdiction.

And as my predecessor, Conrad Harper said at the time, this is a dual requirement that establishes that treaty obligations apply only if both conditions are satisfied. An individual must be under United States jurisdiction and within United States territory.

And now the negotiating position of the United States of the treaty confirms that interpretation. The phrase, within its territory, was added at the request of the head of the U.S. delegation, Eleanor Roosevelt at the time in 1950. And she explained that, quote, the purpose of the

proposed addition is to make it clear that the draft covenant would apply only to persons within the territory and subject to the jurisdiction of the contracting states.

There was a vote held on that addition and that addition was adopted 8 to 2 in 1950. Subsequent efforts to change that have failed.

And again, in his statement to the Human Rights Committee in 1995, Conrad Harper explained that the words were added, quote, with the clear understanding that such wording would limit the obligations to within a party's territory.

Now it's true, and I know that Laura Pitter is going to talk about this, that the Human Rights Committee and a lot of human rights groups in other countries don't agree with the long-standing U.S. interpretation, but the Human Rights Committee's statements don't have binding legal effect on the United States or to any other country. We give respect to them but they're not binding on us.

Both the Bush and the Obama administrations have confirmed the Clinton administration's position that the ICCPR does not apply extra-territorially.

In fact, just five days ago in Geneva we were making our periodic report to the Human Rights Committee and the acting legal advisor, Mary McLeod, told the committee, quote, the United States continues to believe that its interpretation that covenant applies only to individuals both within its territory and within its jurisdiction is the most consistent with the covenant's language and negotiating history.

So we really have fifty years of U.S. practice on this point recently reaffirmed by the Obama administration.

But even if the ICCPR did apply extra-territorially, the treaty would still not place limits on NSA surveillance because persons in other countries are not subject to U.S. jurisdiction.

The Human Rights Committee itself has

defined the phrase subject to a party's jurisdiction to include people within the power or effective control, or effective control of the forces of a state party acting outside its territory. So not even the Human Rights Committee is suggesting that everybody who may be subject to NSA surveillance is actually within the power or effective control of the United States.

And I would want to hear more from my colleague who I've met before, Professor Sieber, but even if they're unhappy with NSA surveillance, I am not aware of any foreign government that believes that the ICCPR or any other provision of international law imposes an obligation to respect the privacy rights of non-citizens.

In fact, candidly, most foreign governments spend lots of time spying on foreign citizens. So they may be unhappy with what we're doing as a policy matter, human rights groups may suggest that there are binding legal norms, but I'm actually not aware that foreign governments are suggesting that there is an actual violation

of international law.

And finally, just to close on my analysis of the ICCPR, and then I'll wind up, even if the ICCPR did impose certain obligations on United States extraterritorial conduct, even if people outside the United States were considered to be within the jurisdiction of the United States, Article 17 of the ICCPR still only bans, quote, arbitrary and unlawful interference with privacy.

Now we can certainly argue about constitutes arbitrary and unlawful interference but there is no international norm on that point. I'm sure lots of people can suggest that the NSA program is arbitrary, that it's unlawful, but when we're talking about international law there has to be actually a specific norm that people have agreed to, and there is no generally accepted framework under international law that defines what kind of surveillance is unlawful or arbitrary.

So the bottom line, despite statements

that we are violating the Article 17 of the ICCPR, it just simply does not apply, nor does any other provision of international law.

And so let me close by saying that just because international law doesn't actually create a universal right of privacy that's binding on the United States, I'm by no means saying that we ought to be insensitive to the rights of non-citizens. Certainly if I were still in the White House I would be saying, you know, we need to be respectful of concerns both of individuals or of leaders. That's why we make these policy decisions.

President Obama's recent presidential policy directive states that signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information.

So it's perfectly appropriate to take

into account privacy interests, but international law does not place binding legal obligations on us. Thank you.

MR. MEDINE: Thank you. Mr. Garfield.

MR. GARFIELD: Thank you. Thank you members of PCLOB on behalf of fifty-six of the most dynamic and innovative companies in the world, thank you for inviting us to testify today. And thank you as well for your efforts to advance both national security and civil liberties.

From our perspective we have the firm view that those two concepts are mutually reinforcing and in fact are not mutually exclusive and so we want to do whatever we can to support your efforts.

I'd like to focus my testimony on two areas. One, what we're experiencing in the marketplace as a result of the NSA disclosures and, then share some solutions that may help remediate some of the challenges that we're facing.

On the first, the economic impact from

the NSA disclosures are significant and ongoing. The folks in this room are very familiar with Section 215 and the distinction between that and Section 702, but for folks outside of this room much of what they experience and what we're experiencing is diminishing trust, particularly diminishing trust in U.S.-based technologies. So rather than made in the U.S.A. being a badge of honor, it's increasingly becoming a basis to question the integrity and security of technologies.

That has a real world economic impact. In fact, there are a number of analyses out there that put the numbers of the impact in the tens of billions of dollars.

As significant, perhaps even more significant than the economic loss is the broader societal impact and the implications for the Internet more generally. We're celebrating this year the 25th anniversary of the commercialization of the Internet and are all very familiar with the benefits and the way it's transformed all of our

lives.

Increasingly, what we're seeing though are policies aimed at changing the open, ubiquitous, globally-integrated Internet into one of walled silos. And so the legislation that's actually being debated today in Brazil would create walled gardens around their data.

And it's not simply limited to Brazil. We're seeing the same in Europe, as you all know, where the parliament is questioning the continuing viability of the safe harbor, or in particular territories within Europe where they're calling for country-specific clouds that would again create these islands of walled silos rather than an open, integrated Internet, which we all know the implications of that.

And so what do we do about it? I'll offer up three sets of solutions that build on global principles that we released earlier this year after working with our members to forge consensus on it.

And I place the emphasis on global

because we firmly believe that in order to address these issues and to address them effectively, high level, global communication and engagement around surveillance is critically important.

The first aspect or screed of solutions is around transparency. This body, the PCLOB in its January report made the point that transparency is the foundation for democratic principles. We firmly agree. We also think it's the foundation for separating fact from fable.

And so to the extent that there's a greater awareness, particularly around 702 where there are protections in place already, for there to be greater awareness about that would be quite helpful.

As it relates to our companies, the ability to share with the public more about 702 and 215 and the requests that come in pursuant to those, as well as the accounts, particularly the numbers, would be incredibly helpful. And so greater transparency is one element of what we would recommend.

The second relates to oversight. And as I've said in other places, including my testimony on the hill, our solutions are offered with a great deal of humility because we don't know what we don't know. I don't pretend to be able to offer the exact framework for making sure that there is a civil libertarian advocate or a civil liberties advocate within the FISA or FISC court process. But developing a framework for enabling that, we think is very important.

Finally, the last set of solutions are based on working to rebuild the trust that has been eroded, and there, a few unequivocal statements from our government would be quite helpful.

By way of example, there has been a lot of reporting around steps that may or may not have been taken to undermine encryption standards. NIST has been very firm in taking steps to make sure that they bolster the encryption standards that are being developed.

But a statement from our government

that they don't, do not intend to take steps to undermine the integrity of our cyber -- to undermine the integrity of those standards would be incredibly important.

Similarly, taking steps to affirm that data acquisition pursuant to 702 is not being done in an indiscriminate manner, I think would also be incredibly helpful. With that, I'll pause.

MR. MEDINE: Thank you. Ms. Pitter.

MS. PITTER: First, thank you very much for this opportunity. Thank you for having me. We've filed a more lengthy statement with the Board so I'm just going to be a little bit more brief here.

I was asked to talk about U.S. obligations under the International Covenant for Civil and Political Rights so I'll start with that.

And obviously, I'm going to disagree with Mr. Bellinger on this issue, as did Harold Koh's recently released memo where he disagreed as well and tried to get the Obama administration to

take a different position, arguing that it was not actually in the U.S. interests to continue to not apply the ICCPR in an extraterritorial manner.

There has been debate about whether or not this treaty applies outside of U.S. borders and it stems from, as Mr. Bellinger said, the operative jurisdictional clause in the covenant which says that states have an obligation to respect and ensure that those within its territory and subject to its jurisdiction, the rights under the covenant.

So the word jurisdiction in that clause has been interpreted to mean power and effective control. But the U.S. does not accept that. It takes a strictly territorial stance. And this essentially means that a state has to abide by the covenant within its territory but then it can willfully violate the covenant outside its territory, killing and pillaging at will outside its borders, which doesn't really make any sense.

Treaty law requires that the language of the treaty be interpreted in accordance with

its context, as well as its object and purpose. And the context in this case was post-World War Two when the treaty drafters were aiming at empowering people with rights universally and not diminishing them, and responding effectively to Nazi atrocities.

To interpret the treaty in that limited way would allow, for example, Nazi Germany to run a concentration camp in Poland, as Marco Milanovic, a prominent scholar on this issue has pointed out.

And the U.S. is the clear outlier on this. Only the U.S. and Israel take such a strict interpretation of the treaty.

So how does this apply to surveillance and the right to privacy? Some have argued that even if the ICCPR applies extra-territorially it should only be in the case where the government has physical control over the individual, like in the context of detention or torture. And that doesn't apply to surveillance simply because the individual is not within a state's effective

control.

But the problem is that their communications are. And so to not recognize even a duty to respect the right to privacy in this context creates a kind of absurd situation where the U.S. would be barred from going into someone's house in Germany and taking letters out of someone's drawer but not barred from reaching into their computer and doing the very same thing remotely.

These are novel questions, and I won't deny that. The Human Rights Committee, which is the main interpretive body of the ICCPR, has not adjudicated this matter.

And though there is a body of case law in other jurisdictions, particularly in the European Court of Human Rights, that have the issue and they do provide some guidance on a framework for how to analyze surveillance laws.

That said, those decisions, they came out before the Snowden revelations so they're not informed by a lot of the information that's come

in the public domain about the vastness of the collection that's going on.

But these issues are novel in the U.S. too. Just because there may not be necessarily a case en point does not mean the obligations or the rights don't exist. They are in the treaty.

Just as like many in the U.S. have argued that U.S. law has to catch up with technology and recognize a reasonable expectation of privacy in metadata, international law has to acknowledge that when it comes to surveillance, though an individual may not necessarily be in a state's physical control, their communications are, and the right to privacy can be violated remotely through technical means.

But just because the obligation applies extra-territorially does not mean that the surveillance has to stop. There is a framework within which surveillance can take place, but also be in accordance with human rights obligations. The surveillance has to be lawful and non-arbitrary and necessary to a legitimate cause

that's proportional to that legitimate aim.

By all accounts, that's not what 702 is. 702 may all be for the purpose of protecting U.S. national security, which would be a legitimate aim, but are there more narrowly tailored ways to achieve that aim?

And if the answer to that question is no, and I'm going to quote from the review group here, the question is not whether granting the government authority makes us incrementally safer but whether the additional safety is worth the sacrifice in terms of individual privacy, personal liberty, and public trust. And also, is it really worth the other harms that will result?

We're in a situation now in which countries are rushing to enact laws that would localize data collection and companies are rushing to offer alternatives to customer data being stored in the U.S.

And from a technological standpoint data flows are not necessarily based on geography but travel the cheapest, most efficient route.

This means a transfer to someone in the same country can mean data passing through many countries without the sender even knowing it. So a failure to respect the right to privacy extra-territorially imposes, exposes U.S. data to vulnerability when it's situated in other states.

The President has already essentially recognized all this. His presidential policy directive purports to bring the rules on retention and dissemination of data collection on foreigners closer to those that govern data on U.S. persons.

But it did not end bulk collection and specifically exempted data temporarily acquired to facilitate targeted collection.

Also, this was through an executive order not legislation, so it could be changed by future administrations.

The bottom line is that the U.S. is in a unique position because most of the world's data flows through its borders. And this confers an obligation to respect the privacy rights of those individuals whose communications fall within the

U.S. jurisdiction, but also to refrain from interfering with the ability of other countries to protect data, protect their own citizens' data. And a failure to recognize the value of this undermines U.S. business and long term national security interests.

The administration says it will make some changes but the law remains the same and that too has to change.

MR. MEDINE: Thank you. Mr. Sieber, Professor Sieber.

MR. SIEBER: Thank you very much for your kind invitation. It's a pleasure to be here.

International legal obligations for U.S. surveillance programs for which you are asking can be based on two different sources, interests of states and interests of persons. The two are interrelated since the protection of a state's territory also has effectual protective functions for its citizens.

Let me start therefore with a few remarks on this broader approach before turning to

specific human rights, which have been addressed here.

General international law and Article 2 of the U.N. Charter protects the sovereign equality and territorial integrity of all states.

A state therefore violates territorial sovereignty if it accesses, copies, or manipulates non-public data in computer systems located in a foreign state because such acts initiate in data processing on the servers located in a foreign territory.

There are no norms in public international law that permit violating other states' sovereignty by across the board world-wide surveillance.

There is also no customary rule of international law that permits the infringement of sovereignty resulting from acts of espionage.

In addition, espionage committed from the premises of embassies violates the obligations under Article 3 of the Vienna Convention on Diplomatic Relations.

These infringements of the territorial integrity of many states by large scale surveillance programs have two impacts for our topic. First, with respect to policy considerations, infringements of the territorial integrity of foreign states violate international law, plus in addition also national cyber crime statutes that are globally agreed upon in the Budapest Convention.

These violations pose serious threat to the continuing trust and the integrity of the U.S. and its IT industry. This infringement may be more serious than the violations of privacy rights, the scope of which are controversially in dispute in most countries.

Secondly, transnational surveillance programs on foreign territory take over the security functions of the affected states. This transnational control deprives citizens of protection by their own state and any other legal protective systems in these security measures, since their home state cannot protect them against

unknown foreign violations of their privacy and the intercepting foreign state often does not recognize any aliens' rights outside its territory where the interception is taking place.

In such a global system the citizens, including U.S. citizens, are deprived of any protection, especially if authorities of different countries exchange certain data.

Thus we are all losing a protective system which mankind has won in a long historical battle dating back to the Enlightenment. Thus, if we are engaging in transnational surveillance programs we must at least recognize certain basic human rights apply to all humans, regardless of nationality and place of residence. And if we want to create an effective global solution this must be supported by international human rights, to which I will now turn.

In the field of international human rights I will also concentrate on Article 17 of the International Covenant of Civil and Political Rights. The International Court of Justice, the

U.N. Human Rights Committee, both in its case law and in its General Comment 31, as well as many national courts and governments acknowledge the extraterritorial applicability of the ICCPR.

I also simply refer to the well-founded memorandum presented by Harold Koh, former legal advisor at the U.S. State Department in 2010 and 2013, with respect to the ICCPR. Koh is convincingly for the extraterritorial applicability of the conventions.

According to the prevailing opinion, the ICCPR is extra-territorially applicable to anybody within the power or effective control of the acting state party or its agents.

In the physical world, extraterritorial applicability of the ICCPR is thus limited to situations in which the government has total or special control, spatial control over a territory.

Since communications and privacy rights are by their very nature exercised in the virtual world and are prominently infringed upon there, the control of this virtual world by highly

extensive surveillance programs should be a decisive factor.

If we do not accept these conclusions we still must deal with an argument of the German Constitutional Court, which also might be relevant for the American discussion. The court argues that telecommunication interception not only infringes upon privacy rights by the first act of recording the telecommunication, it also infringes on these rights by the following data transmission to their home country, the analysis, the linking, the long-lasting storing, and by further transmissions to other recipients.

All these acts are repeating and deepening the infringements of privacy rights and they are undoubtedly committed on the territory of the surveilling states. Thus, even in cases of foreign intelligence gathering, we are not dealing only with actions outside the national territory.

Accepting the arguments for the transnational applicability of specific international human rights would promote then a

deeper discussion on the substantive scope of international human rights protection of privacy.

A first attempt to define the contours of the international concept of privacy can be seen in the already mentioned U.N. General Assembly Resolution 68167 of last December on the right to privacy in the digital age.

When this discussion proceeds, it will be most important to recognize that threats from abroad are different from internal threats. Thus the principle of proportionality as developed by international and national courts will lead to very different results in different circumstances, such as for data collection to homeland, in Afghanistan, or today in the Ukraine.

These necessary differentiations under the principle of proportionality can recognize many U.S. security concerns. Thus applying certain transnational privacy rights would not prevent a reasonable security policy, especially also since the ICCPR is self-executing in the U.S.A. and national foreign citizens could not

initiate judicial proceedings against the U.S.

In sum, I would advocate for an international solution and discussion in order to maintain or regain the leading role of the U.S. as an advocate for the rule of law and human rights in democratic societies, as well as for the trust in its IT industry and its clouds.

If time is not yet ripe for an international human rights solution, then more emphasis should be placed on national efforts to provide more guarantees for non-U.S. persons.

For that reason I welcome the respective U.S. Presidential Directive 28 of last January to applying certain safeguards for all individuals, regardless of the nationality of the individuals to whom the information pertains or where that individual resides.

This policy is also the position of the German constitutional law. In case of your interest it would be a pleasure for me to provide you with more details on these comparative legal aspects later on in the discussion. Thank you.

MR. MEDINE: Thank you. Mr. Wolf.

MR. WOLF: Thank you, Mr. Chairman. As Chairman Medine said at the outset, I'm the partner in the law firm of Hogan Lovells, where I lead the firm's global privacy practice.

And in 2013 Hogan Lovells published a white paper examining the similarities and differences among various legal regimes that authorize and limit governmental access to data.

And our work began before the Snowden NSA disclosures in response to the claims of certain EU cloud service providers that storage of data in the EU made it safer from surveillance than storage with a U.S.-based cloud provider.

Obviously following the Snowden revelations the argument in support of allegedly secure from surveillance regional clouds has been renewed loudly.

A previous white paper we did on governmental access to data internationally noted the availability of mutual legal assistance treaties and other forms of cross-border

governmental sharing addressing faulty claims of regional cloud service providers about the invulnerability to foreign government access that local cloud storage might provide.

Our 2013 white paper specifically looked at Section 702 surveillance and the frameworks in Australia, Canada, France, Germany, and the United Kingdom. My written and oral testimony today synthesizes the findings from this white paper and includes additional information on similar laws in Brazil, Italy, and Spain that we intend to publish soon.

I will note that our white paper foreshadowed last week's report of the European Parliament criticizing the practices of certain EU member states for the lack of transparency and controls on their surveillance activities.

My principle point today following our white paper is straightforward. While the policies and practices of the United States addressing surveillance and related privacy concerns obviously need to be and are being

reassessed, the U.S. has on its books greater due process and independent oversight of surveillance activities than many of our fellow democracies.

As you know, Section 702 surveillance requires court approval, surveillance is limited to foreign intelligence information, and oversight mechanisms exist for 702 surveillance.

As our white paper revealed those same limitations are not always found in the law of many of our counterparts. Australia, Canada, France, Germany, Italy, and the United Kingdom do not require court approval for national security surveillance.

In France, the intelligence agency is allowed to conduct surveillance to protect economic and scientific assets, even when national security interests are not at stake.

On the issue of intelligence agencies secretly and without any process at all asking companies for data, we have found that Australia, Canada, France, Germany, and the U.K. allow their governments to ask private entities voluntarily to

disclose data to the government.

In the U.S. the government is not allowed to seek voluntary transfers. A neutral judicial body must approve the government's request for data.

Last week's resolution by the European Parliament recognized extensive surveillance systems in EU member states, and the lack of control and effective oversight that some EU member states have over their intelligence community.

The resolution also questioned the compatibility of some member state's massive economic espionage activities within the EU, with the EU internal market and competition laws. The parliament did not go into the detail of our white paper, but its resolution reflected the baseline findings of our research, that there are substantial deficiencies in transparency about and controls over national security access to data in countries outside the U.S.

Thus when also considering the cross-

border sharing arrangements available to governments for information they collect through surveillance, it is misleading in the extreme to contend that so-called regional clouds provide individuals with security from government surveillance.

I commend this Board for engaging in an assessment of U.S. surveillance practices and looking at how these practices relate to our counterparts. There are no guarantees in the U.S. or elsewhere that agencies will abide by the laws restricting national security surveillance, but the degree of authorization required and the kind of review that occurs is obviously relevant to a determination of how well personal privacy and personal liberty are protected.

Thank you again for the opportunity to present the findings of our white paper and I'll look forward to your questions.

MR. MEDINE: Thank you very much.

I want to turn to the ICCPR for a moment, and as I understand it there are really

two issues here. One is the jurisdictional test, and if you pass that then the substantive test with regard to evaluating whether the 702 program affords appropriate protections or is arbitrary in some fashion.

I want to start with the jurisdictional issues, and that is, I guess there are three interpretations of the applicability of the treaty. One is that there has to be both territorial presence and jurisdiction. The other is there could be one or the other. And I guess the co-approach, which is they sort of split it, and that is there is a respect requirement across the board and an ensure requirement only subject to the territorial and jurisdictional issues.

I want to ask about the jurisdictional side. As we know from discussion earlier today and what's been made public is the information that's being collected under the 702 program is being collected in the United States, albeit about non-U.S. persons.

I guess my question is for the

panelists, how should we, how should one interpret jurisdiction? It's not going to be up to us to interpret it, but in terms of understanding jurisdiction, is it jurisdiction over the information, which may be here, is it jurisdiction over the person, who may be elsewhere? And how would that apply, both in sort of friendly and unfriendly countries, in terms of the scope of our responsibilities?

MR. BELLINGER: I'll take a stab at that. Let me say a couple of things. One, just to reiterate that the U.S. has in fact reaffirmed its position again that the ICCPR does not apply extra-territorially and the point that the individuals have to be under the power and control.

You know, I get sort of the novel suggestion that anybody who is subject to electronic surveillance is therefore under U.S. power and control. But I don't think that's actually a credible argument.

Even the Human Rights Committee I think

would not go so far as to say that if one can touch a foreign national through surveillance that that is someone who is under U.S. power and control.

The fact that the surveillance may be then collected ultimately inside the United States I think does not change the fact that the collection is being done of persons who are outside the United States. And so I think that does not change the, either the essential jurisdictional element that it does not apply extra-territorially outside the United States, and that those individuals are within the power and control of the United States.

Again, these are things that one might wish were so, and I'm not sure that there's as much of a disagreement between me and Laura Pitter as she suggests.

If one were writing a new treaty and could get people to agree to certain things one might agree that there might be, you know, policy limitations that one might accept.

But the way this particular treaty is written now, certainly the view of the United States government, and I frankly think I am not aware of any single government in the world, and I mean this is what I mean, governments who believe that their right to conduct electronic surveillance of people outside their territory is controlled by the ICCPR. I would be very surprised if we found any European government, as upset as they might be with electronic surveillance by the United States, who would say the Article 17 of the ICCPR limits our ability to collect outside our borders.

And in fact, the German government in a submission made to the European Court of Human Rights interpreting the European Convention on Human Rights argued that that convention did not limit its electronic surveillance of Uruguayans outside of Germany.

So again, the view of governments is that this does not have jurisdictional control over people who are outside their territory.

MR. MEDINE: I just wanted to follow up. What is the scenario where someone would be in our territory and not within our jurisdiction? Because the statute, the treaty says both territory and jurisdiction. Are there other situations where one would apply but not the other?

MR. BELLINGER: Well, certainly there would be people who would be, theoretically there could be people who are not in our territory and who could be subject to our jurisdiction. That was the problem that Eleanor Roosevelt was trying to solve at the time, to think about what the converse might create.

MR. MEDINE: Okay, thanks. Ms. Pitter.

MS. PITTER: Well, first of all, the German position was taken in 2008 before these revelations came forward and they've since sponsored a U.N. resolution which underscores the importance of respecting the right to privacy.

So I would say that, you know, Koh's interpretation is that there's on the one hand a

duty to ensure the rights in the covenant to those within a state's territory and jurisdiction, and then there's also a duty to respect the rights of individuals outside of the territory, the actual territory of the United States.

So there's the duty to respect is what's important here, and so there is an obligation under the ICCPR, even with the jurisdictional clause, to respect the rights to privacy of those outside the United States.

But this all, as you said, is happening in the United States. I mean the data is flowing through U.S. borders, although I'm not sure about the backbone upstream collection, where exactly that's taking place. So absolutely, yeah, absolutely, I mean I think that it would be the duty to respect the right to privacy is what's implicated here.

MR. MEDINE: Thank you. Judge Wald.

MS. WALD: I've got two questions I think for Mr. Bellinger. First is I think we recognize that the government has now reaffirmed

its earlier position about what the ICCPR means in relation to people abroad. But I wondered if you'd just say a word about how they dealt with the question of Article 31 of the Vienna Convention on the interpretation of treaties insofar as, as I remember it, you know, deference should be given to the official interpreters of the -- which in this case I believe, you know, have taken a much broader interpretation of that.

And I think a couple of our Supreme Court justices have said in several cases that when you're interpreting, when they're interpreting a treaty one should look to the interpretations, maybe for guidance, maybe not controlling, of other parties to the same treaty. Just a word or two on those two aspects of the reasoning which led to what is, is the reaffirmance of it.

MR. BELLINGER: Right, and I think what you're talking about is the General Comment 31 of the Human Rights Committee.

MS. WALD: Yeah, yeah.

MR. BELLINGER: Which certainly in the view of the United States, and again, I'm not aware of any government in the world who believes that the views of the Human Rights Committee actually are legally binding.

The Human Rights Committee was set up to monitor compliance and it makes statements which governments, including the United States, give respect to but we certainly don't, neither we nor other countries believe that that is the definitive interpretation of the treaty, nor do we believe that it's legally binding.

MS. WALD: Okay. My second question --

MS. PITTER: I was just going to add, sorry.

MS. WALD: Go ahead.

MS. PITTER: That it is, the Human Rights Committee is a very authoritative source regarding the interpretation of the covenant. And I mean the U.S. is under an obligation to give effect to the rights in the treaty in good faith. So what the Human Rights Committee has said in

that regard is very important.

MR. BELLINGER: And if I could just say, because these are important points right now, including for treaties, frankly the Human Rights Watch is extremely interested and having gotten through the senate the U.N. Convention on Disabilities.

So you know, Human Rights Watch can speak for itself, but certainly the view of the U.S. government and of most human rights organizations is that the statements made by these treaty compliance groups, while due great respect, are not binding on the United States.

If they were in fact considered to be binding on the United States, those would in fact fundamentally change U.S. obligations under the treaties and we would never get any treaties through the senate, including the treaty that both Laura and I would very much like to get through the senate, the U.N. Disabilities Convention.

MS. WALD: Okay. My second question very quickly is that acknowledging what

everybody's about, that this big debate in the international world will continue probably despite the most recent position we've taken, and given, you know, all of the people allied with it, the official interpreters, whatever they're called, Harold Koh, Sara Cleveland, Manfred Nowak, who's the U.N.'s leading expert on the ICCPR, my question to you deals with the last paragraph of your both oral and written testimony, and that is that you would see no problem with a policy which gave greater consideration to the rights of non-U.S. persons within the surveillance context, alluding to the fact that the President in his directive suggested that.

But I'm wondering if you, having served the position you did as counselor in the State Department, have any more specific ideas about in this context 701, or maybe even in other surveillance programs we could do just that?

MR. BELLINGER: Thank you, Judge. It is a great question. I have not actually given a lot of thought to that.

MS. WALD: Maybe a little.

MR. BELLINGER: My general sense from the surveillance that I saw was in fact that we are very targeted on specific intelligence requirements.

These are not broad dragnets of the surveillance of average individuals and so this is not a great violation of the rights of privacy of every single foreign national, that's very much focused on individuals who may pose a national security threat or for which the United States has a valid intelligence interest.

MS. WALD: Would you, for instance, think that taking national security, assuming you didn't have a national security risk, that basically non-U.S. persons we should try to approximate as much as we can within those restrictions the equal treatment in use, retention, that kind of thing of non-U.S. persons in our surveillance, or not?

MR. BELLINGER: I think that some of the things that the Obama administration,

President Obama has been focusing on to ensure that, particularly for the information that is collected, that we ensure that it is kept private.

I mean I would be personally, I haven't seen this happen, but I would be personally extremely concerned if we found that the United States had collected information about foreigners great or small, either a world leader or a lesser known person, and then we're not careful with that information and were to let it out. That would very much interfere with that individual's right to privacy.

I think, you know, as a national security official it's important for us to collect the information that we've collected, but we need to be extremely careful with it. So my sense is that as a policy matter these privacy concerns are important.

MR. MEDINE: Mr. Dempsey.

MR. DEMPSEY: My question I guess for Laura Pitter and maybe also for Mr. Sieber. Among the major, certainly the countries that Chris Wolf

looked at and cited, but among the other major democracies that do foreign intelligence surveillance, is there anyone that has a law which you would point to as a better model?

MR. SIEBER: Could you ask the question?

MR. MEDINE: Is there a country that has a better model of surveillance than ours? Is that --

MR. DEMPSEY: Yeah. In other words, what other country has a better model, a better law, more checks and balances, more controls, more limits?

MR. SIEBER: In general.

MR. MEDINE: In general, checks and controls balancing privacy and civil liberties and national security.

MR. SIEBER: It's a very broad question --

MR. DEMPSEY: Just pick one.

MR. SIEBER: Because you have to consider many, many aspects, not only the

extraterritorial implication. I just can give you some reliable differences a between the German system and the U.S. American, that's what I can witness on.

If you have a look at the German system you have to see that Germany has a very strong constitutional court and is very much attached to fundamental rights. This is a reaction to the Nazi cruelties and any steps towards this direction should be prevented. This is the reason for some very basic differences between the U.S. and Germany.

The first one, for example, is that intelligence agencies in Germany have no executive powers. So they cannot execute arrest warrants or anything like that. They just can collect the information. This is based on the idea that the lack of control which we have in this area of intelligence agencies must be balanced by lesser constrained measures.

Secondly, Germany has constitutionally founded strong separation of powers and separation

between the police and the intelligence agencies. This has been changed a little bit after 9/11 but still there is a fundamental separation.

Information exchange is only possible in a very limited way for very, very serious, serious crimes.

So I would say the differentiation between the institutions is stricter. We don't have multipurpose institutions like the FBI.

On the institutional side there is an absolute strong separation between these institutions, despite certain common datas and things which we have done after 9/11.

You could go further, if I compare it and look around at the control agencies which you have. In Germany it's separated. For internal surveillance we have a special commission appointed by the parliament, G-10 Commission who is doing the job. It's not called a court but the functions are similar.

And for foreign intelligence agency, the BND, there is a parliamentary commission who

does these things.

Maybe one last point, if you look at the aspect of protection of foreigners' rights and applicability of the constitution abroad, the German attitude is more in favor of applying the national constitutional guarantees.

With respect to the first question, which is foreign territoriality, section 1 of the basic law says that the basic law binds all public authority. And this is in general irrespective of whether it's in the country or outside the country.

There are differences of course, but they have more to do with the different circumstances, because the risks coming from abroad might be bigger than coming from within the countries, and for that reason I absolutely agree that the systems might be different for internal intelligence and external.

But it's not based on the fact that we do not apply the constitutional guarantees abroad, and it's definitely not based on the fact that we

are giving different rights to foreigners and to citizens, at least in this area of dignity rights, of human rights, and especially in the privacy rights.

So for example, there was a German decision of the court which was controlling intelligence gathering for abroad and which checked these systems.

So with respect to this question which we are dealing here, if I generalize it I would say we are more open to applying these fundamental rules. We do not reject it as it's not applicable. We don't go into these (inaudible) stay out of it. We would apply it, but then we have a proportionality principle and we check whether the things are justified.

And for example, in this decision I mentioned, the court said, yes, dangers coming from abroad are bigger, bigger dangers, and with balances and this law was in general justified with one exception.

It was applied also by law to internal

conflicts, and the constitutional court said it cannot apply just like that.

So I think these are the main interests which I could tell you. It's impossible to say better or worse. I would never, never do that.

MR. MEDINE: Thank you. Ms. Cook.

MR. DEMPSEY: We'll come back around.

MR. SIEBER: And if you permit afterwards I would like to say a few words with these International Convention 17, the applicability, but I don't want to --

MR. MEDINE: We'll come around at the end.

MS. COLLINS COOK: So I wanted to thank you all for coming and to congratulate you for being the panel that has come the farthest set of distances to participate today. I think it's very helpful to have this type of discussion in an open forum.

We've talked a fair amount today and all through the day about skepticism about U.S. law and U.S. practices. I think it's fair to say

there is also a high degree of skepticism about the contours -- let me get closer here.

I think it's fair to say that there's a high degree of -- if I can get through this question without hurting someone, this is really going to be my goal for the day.

(Laughter)

MS. COLLINS COOK: There's a high degree of skepticism about the contours and applicability of international law as well. So having experts who are able to speak to these issues is critical, I think, to us.

And I wanted to draw off of something, Professor Sieber, that you had mentioned and I have to confess it was not a focus of mine coming into today. I had been focused on the ICCPR and the potential applicability of Article 17.

But you talked about the interests of states, and if I understood what you said correctly, that the interest of a state in its own sovereignty is inviolate, that surveillance by one country in another country is a violation of that

sovereignty, there is no exception under customary international law that would make that any less of a violation of the state's sovereign status or rights.

So that's the academic point. That would lead me to think that no one was conducting surveillance on anyone else, that no country is doing surveillance.

But as a practical matter I think it's fair to say that every country is either engaging in foreign intelligence collection or attempting to engage in foreign intelligence collection.

So if you can explain to me how you can have a principle of customary international law, here the absence of an exception that is honored by not one country in the world, as I understand it.

MR. SIEBER: Yes, I remain with the saying that there is no permission of espionage under international law because the principle of self-defense, that needs an armed conflict for it. It's not there for the ordinary case.

And customary law would require an opinio juris, the conviction of the people that espionage is right.

But our estimations, that are split. If we are considering our own law, we say, yes, we do it and we give them a medal if they are successful. If we are considering the other, we say it's illegal.

So there are two regimes of law which come to different results. We live with that but we cannot say that international law has a general view that we can, that we can do it.

We have this problem in a very interesting case with the German reunification because when the two parts of Germany came together, there have been people doing espionage in East Germany and they are now under our jurisdiction.

This question came up and here again the Constitutional Court said there is no general violation of international law, and I think you agree with that. We have to live with this

conflict.

And in the global world that's normal. The world is getting so diverse that we have many conflicting regimes today now, so we can stand with that.

MS. COLLINS COOK: So I guess my question, perhaps Mr. Bellinger, you can speak to this, is it a violation of international law in terms of infringing the interests of another state to engage in sort of foreign surveillance?

MR. BELLINGER: I was going to jump on that as well. And the answer to that I think is clearly no. I am not aware of any country who believes that the U.N. Charter's statement on the protection of territorial integrity and sovereign equality of states actually prohibits electronic surveillance of another country.

Certainly if that were the understanding of our senate that in becoming party to the U.N. Charter that prohibited us from spying on another country because it would violate their sovereign equality or territorial integrity, then

we would get out of the U.N. Charter immediately. But I am not aware that any other country believes that as well.

So there is not, the principle of territorial integrity and sovereignty would apply to, say, for example, use of force. International law does not prohibit electronic surveillance or spying. Domestic law may.

And so that's really, you know, when we talk about international law, that basically means that there is a compact between countries. Judge Wald knows this very well, you know. Countries have to have agreed that they are not going to do these things to each other.

And in the U.N. Charter, the U.N. Charter was not saying we promise not to spy upon one another, we were saying we promise not to use force against one another.

U.S. surveillance in another country might violate the other country's law, but it is not a violation of international law.

MR. MEDINE: Let's go on to another

question. We'll give Ms. Brand a chance and then we'll come back.

MR. SIEBER: Because I think I have to contradict.

MS. BRAND: All right. Let's see if this microphone will work now.

Thank you all for being here today. One of the things I find frustrating about this discussion, not here specifically but in general is that there is a tendency to not distinguish between what is law and what is -- it's not working is it?

And what is either what people would like to be the law or what is a matter of policy.

And John, thank you for making that distinction very clearly in your remarks.

I was having a little bit of a harder time, Laura, following where you were moving from what you think is actually binding law to what is not.

And so I wanted to know if we are looking, setting aside policy, aspirational policy

for a moment, if we were trying to determine whether what the government is doing under 702 is legal, do you think there is some binding international law instrument that affects that questions?

MS. PITTER: Yes. I mean from my position it is a violation of Article 17 of the International Covenant on Civil and Political Rights. The United States does not recognize that, and that's part of the problem.

MS. BRAND: So let me just ask a question then. If the U.S. government doesn't recognize that, what is the body, what is the document, what is it that then makes that law binding on the U.S., on the agencies implementing 702?

MS. PITTER: It's the treaty itself. As Mr. Bellinger said, you know, a treaty is something that governments have agreed to abide by and to honor the commitments in the treaty in good faith.

MS. BRAND: And what is the body that

has the last say on the interpretation of the treaty, right? Because obviously the U.S. government interprets the treaty differently from the way you interpret the treaty.

Is there some other body besides the U.S. government itself whose interpretation of the treaty is then binding on the way the U.S. agencies implement it?

MS. PITTER: Well, the Human Rights Committee is one of the most authoritative sources on this, but --

MS. BRAND: But is it legally binding, right? That's my question, not is it persuasive, is it binding?

MS. PITTER: I mean from the opinion of many other governments it is. The treaty is binding upon them. The United States does not recognize the extraterritorial application of it.

MS. BRAND: And this is an honest question, give me an example of a country that views the ICCPR to have extraterritorial application with respect to surveillance of

foreigners abroad that itself that takes its own advice or heeds its own interpretation.

MS. PITTER: So this surveillance, as I said, is a novel issue. It's not something that's been addressed by the case law, and especially not since the revelations from Snowden which have disclosed, I think even to policy makers in many countries, the degree to which the law, the domestic law on the books is actually being applied, and the vastness of the programs, how much data is actually being collected.

So it's a novel interpretation, I mean it's a novel question, as it is in the United States --

MS. BRAND: I'm sorry to cut you off but we have a strict timekeeper here, the Chairman, and I want one last question.

I'm interested in your interpretation of what constitutes control and how being surveilled essentially would put someone within the control.

My concern about that interpretation in

part is that I'm not sure what meaning is left in the phrase, under its jurisdiction. If the statute talks about territory and jurisdiction, if jurisdiction means something in addition to territory, it seems like a meaningless phrase if it can include surveillance.

MS. PITTER: Well, it is meaningless in the sense that the United States has taken up, used the technology to conduct surveillance on a very mass scale. So it affects an enormous number of people.

The, you know, jurisdictional clause has been interpreted extra-territorially in the context of detention and torture, in which a smaller number of people have been affected. But when you're talking about surveillance --

MS. BRAND: But detention, I mean someone being detained or tortured is, I would say, much more clearly within the control of the government who has detained or is torturing them, right?

So my question is when you get into

surveillance and the person is clearly not within the physical custody of the government in question, what is it within the ambit of the treaty?

MS. PITTER: So you can look at it two ways there. You know, their communications are within the effective control of the government and so that's one way to look at the obligation.

But in addition, they have an obligation to ensure the rights within the covenant territorially, but also to respect the rights in the covenant extra-territorially.

So although they are not necessarily bound, you know, to enact legislation domestically regarding, you know -- well, they're not necessarily bound to ensure the rights of individuals with regards to privacy extra-territorially, they are bound to respect those rights extra-territorially.

MS. BRAND: I see my time is up.

MR. MEDINE: Mr. Garfield, in your statement earlier you indicated that the

revelations about the surveillance programs, particularly 702, has had significant international impact with regard to business dealings with U.S. firms, and you proposed a number of steps to ameliorate that, and I wanted to ask you about some of them.

And you also mentioned one of them, namely transparency in your remarks earlier. Do you have thoughts about what level of transparency would be helpful to companies, but taking into account national security concerns?

As you know, our first report on 215 did recommend greater transparency, but in terms of disclosures that a company can make about surveillance requests from the U.S. government, so long as that took into account national security.

And I guess in particular if you have comments on the agreement that was reached between the Department of Justice and a number of firms, whether that agreement goes far enough and provides sufficient detail to give comfort to business partners of those firms overseas.

MR. GARFIELD: Thank you for the question, first of all. The agreement with the Justice Department is viewed as a significant step forward. There are additional steps that can be taken that would be helpful as well.

One is the level of detail that the companies are able to share, including disaggregation of data between Section 215 and 702, or whether it's a national security letter. So a greater level of granularity would be helpful.

The second part of that is it is not only important that the companies be able to share out information but that the government share information as well and provide greater transparency, which is often lost in these discussions.

The debate that's been taking place today speaks to the importance of greater transparency because 702 already includes a number of protections that are not generally known, particularly internationally.

To Christopher Wolf's point, if they were more well-known it would be clearer the extent to which steps are being taken in the United States that are not necessarily being taken in other countries.

MR. MEDINE: And you also recommended, made a couple of other recommendations that you put forward were oversight, the importance of oversight and in discriminant collection.

And I guess the question is in the 702 program isn't there already oversight through the Foreign Intelligence Surveillance Court and some of the internal government processes?

And with regard to indiscriminate collection, I think as we heard earlier there has to be a foreign intelligence purpose, and so it's somewhat constrained. Do you think that with regard to this program it meets those requirements?

MR. GARFIELD: Correct. My recommendations there weren't intended to suggest that it in fact was indiscriminate. It was

suggested, it was a suggestion that taking steps to be clear about the protections that are in place and to the extent it is not, it is in fact not indiscriminate, to reaffirm that would be helpful as we go about doing our business internationally.

MR. MEDINE: And Mr. Wolf, you analyzed other country's laws and shown that they're not only not better but maybe not even as good as our laws by some criteria. What lessons should we draw from that in terms of how countries should conduct their surveillance programs?

MR. WOLF: So the purpose of our white paper and our research was really to be expository than to reach judgements and to pick winners and losers or to decide whose was better or best.

But we thought it was important in light of the claims that were being made, particularly by the cloud industry in Europe that there is national security access obviously that goes on in the EU and elsewhere around the world, and often without the controls and safeguards and

transparency that we have here.

So the overall conclusion that we reached is that this is a global problem. Obviously it's one that has been focused on intensively here in the United States because of the Snowden revelations, but it is an international issue that needs to be resolved internationally, particularly with the sharing that goes on among intelligence authorities.

It is heartening that the European Parliament in its resolution last week adopted the draft report that came out in January that focused on the European intelligence gathering practices.

We hope that the data protection authorities in Europe who've been vigorous critics of the NSA practices will comment on their own country's practices. They've been relatively silent on that, and we think the debate that has to be made should be among all those interested in privacy protection, and obviously that would include the privacy commissioners abroad.

MR. MEDINE: Obviously countries have a

lot of self-interest in conducting surveillance programs. Do you see a forum in which countries can or even should agree with the methods by which they conduct surveillance?

MR. WOLF: So that's well above my pay grade. I really don't have a view on that.

I do have, if I can just mention on the transparency point, we did a white paper in August that then general counsel of the Commerce Department Kerry cited in his speech at the German Marshall Fund that actually showed on a per capita basis access by national security and law enforcement on a per capita basis is larger outside the United States in many instances.

MR. MEDINE: Judge Wald.

MS. WALD: I have two questions for Ms. Pitter. Given what most or many observers concede are widely varying practices in different countries about surveilling their own and other country's citizens, would you advocate, as we sitting here have to make some observations, maybe recommendations on 702, would you advocate that we

unilaterally, we recommend unilaterally putting in place one and the same protections for non-U.S. person surveillance that we have for U.S. citizens? Or two, raising the non-U.S. citizen person protections to the level that the official bodies of these international organizations that we've talked about say they should be?

If you come out on the second, what specific criteria do we have to go on as to what those practices would be?

In other words, there's a slightly cynical end to the question, what would be the additional protections in real time to privacy interests of non-U.S. persons if the U.S. took a position that the ICCPR does apply to our activities outside territorial U.S., but that we've already met those standards, such as seems to be the case with some of the other countries who espouse the official broader interpretation of ICCPR but then go on their way, as Mr. Wolf suggested, and don't really raise those?

MS. PITTER: This is to me?

MS. WALD: Yes, this is to you.

MS. PITTER: So, I mean I think one clear change that needs to be made is the purpose of the surveillance needs to be much more targeted. The definition of foreign intelligence information is just much too broad. It encompasses, you know, things that, conversations that could be just about generally the foreign affairs of the United States.

And I know we heard in the panel testimony earlier that that is somewhat reined in by certifications but those are not public and we've not seen them.

There should be a lot more transparency in the law. I think the difference in the German law is that there is a lot more transparency. The capacity also is less in Germany. I mean the U.S. has vast capacity, so you know it affects a lot more people.

But definitely a more narrow, a more targeted approach, and applying, you know, necessary and proportionate principles to the

surveillance as well, I think would go a long way.

There's probably plenty of room for recommendations. I probably can't get into all of them here but that would be --

MS. WALD: In general would your standard be that there should be a presumption that we treat non-U.S. persons like U.S. persons in our surveillance activities, or rather that we go to the best practices we can pull from that people who endorse the ICCPR, even if we don't actually endorse that application?

MS. PITTER: So I think that there can be differences in the law itself but it has to, the differences have to be ones that don't impair the impact of the right itself.

So the right to privacy has to be part of, it has to be made part and parcel of the assurances, but they can be different for practical reasons when it comes to --

MS. WALD: Can you give us, in my remaining few seconds, some application of what you've just said to 702?

MS. PITTER: Well, I'd like to go into, you know, a more detailed analysis here but right now there's --

MS. WALD: Well, just quickly.

MS. PITTER: There's not a warrant requirement, for example, under 702 for individuals, but there should be -- it may be that it's not a practical requirement to have a warrant for individuals outside of the United States.

And it's not just individuals under 702, it's also facilities and about targeting as well.

But the procedures that are in place to protect against sort of suspicionless, you know, there's no standard for what authority has to find before it can target an individual. The main distinguishing principle is that it's a foreigner, and that that information is going to be acquired for foreign intelligence purpose, for foreign intelligence purpose, so that is too broad.

MS. WALD: Okay.

MS. PITTER: Does that make sense?

MS. WALD: Yes. All right, very quickly I guess, Mr. Wolf, your testimony, you know, recited the report about the lesser, basically the lesser protections most other countries including our close allies give to privacy, at least despite some of their countries adherence to the ICCPR's broader definition of privacy, yet you also note that the economic risks to U.S.-based telecommunication companies from threats both from competing companies inside those countries and from the governments themselves that they may balkanize and insist on collection and storage activities being conducted in-country poses a real risk.

Is it above your pay grade to give us some indication of what line or policies the U.S. should follow given those two competing concerns?

MR. WOLF: Well, I think our concern in doing the work that we did on the white paper was the misperception that was arising --

MS. WALD: Let's assume you've done those and that they are real, but also are real

the threats to the competitiveness of U.S. companies if foreign governments and peoples get very excited and want to keep everything inside their own countries.

MR. WOLF: So our position is that they're deceiving themselves if they think that when they keep data presumably within the four borders, four corners of their own country that it's safer from surveillance, not only from their own surveillance authorities, but of course through the sharing arrangements from surveillance authorities from elsewhere around the world, and that the Balkanization of data is not a useful global phenomenon at all.

MS. WALD: Well, what can the U.S., or what could we recommend they bring them together?

MR. MEDINE: Judge, your time has expired. Mr. Dempsey.

MS. WALD: Right. You can think about it.

(Laughter)

MR. DEMPSEY: On my last round we were

talking about what were, if any country's laws that did a better job here, and Mr. Garfield, you were ready to jump in. Do you remember what you wanted to jump in on? I wanted to give you a chance to make the point, if you still remember what it was.

MR. GARFIELD: It really was the point that was made in response, which is that in fact our experience in carrying out our business is that there aren't many, if any, other countries that have as many safeguards in place.

The lack of open discussion through multinational engagement as well as transparency here in the U.S. furthers that false perception that somehow other nations are doing more than we are. And that is certainly something that whether through legislation or recommendations from the PCLOB, we can do something about.

MR. DEMPSEY: The question for Laura Pitter, a couple of other witnesses have raised this and a couple of times I grabbed for the book in order to raise it and didn't get a chance to,

the definition of foreign intelligence, as I read it, it means information that relates to the ability of the United States to protect against actual or potential attack, grave hostile acts of a foreign power, sabotage, international terrorism, international proliferation of weapons of mass destruction, or clandestine intelligence activities. None of those are too broad, I would think.

And then it says, information with respect to a foreign power or foreign territory that relates to the conduct of the foreign affairs of the United States.

I mean isn't that precisely what foreign intelligence is supposed to be about, information with respect to what foreign countries are doing that might affect our foreign affairs? Why is that too broad?

MS. PITTER: I think that the first category of information that you said could, it would be permissible. But the general foreign affairs of the United States allows for the

collection of a vast amount of information that does not necessarily have any national security purpose.

MR. DEMPSEY: No, but it has foreign affairs purpose. It is by definition about the intent of foreign governments, and are you saying that other countries self-restrain themselves from trying to understand what their adversaries are doing, even in matters that don't involve attack and so on?

MS. PITTER: I mean if other country's laws are overbroad and vague then they're in violation of, you know, the International Covenant on Civil and Political Rights as well.

MR. DEMPSEY: Well, I think John would say that if everybody is doing it, it probably isn't a violation of the treaty. Everybody didn't bind themselves not to do what they all were doing at the time they bound themselves to the treaty.

MS. PITTER: Well, you know, the revelations about how this is applied are just coming out now and there are going to be

challenges and there already are challenges to the law.

And I think we're going to find that there is room certainly for reining in the overbroadness of some of the statutes as they exist right now.

I think that because it allows for the communications of things that don't necessarily have to do with national security, that it just, it's overbroad and it's impacting, you know, the United States in other ways.

MR. DEMPSEY: In what way is the collection of information about foreign affairs overbroad?

MS. PITTER: Because it could be, you know, someone talking about, you know, their opinions about the foreign affairs of the United States --

MR. DEMPSEY: Not someone talking about their opinions, it's the information with respect to a foreign power. So this is not Joe Schmoe in Germany saying I like or don't like the United

States, this is about what Germany thinks about the United States.

MS. PITTER: It merely has to relate to the foreign affairs of the United States --

MR. DEMPSEY: Yes.

MS. PITTER: In my opinion it's too broad. It allows in for much too broad a type of communication.

MR. DEMPSEY: No, I'll yield. I'd like to have another round, a third round if we could, but I'll yield for now.

MS. COLLINS COOK: Mr. Bellinger, I think you had put your finger up midway through that and I'd like to follow on this conversation as well because it struck me.

First, where would you draw the line? And I'm struggling to determine what precisely is impermissible about collecting foreign intelligence in the category of foreign affairs as set forth in FISA.

MR. BELLINGER: Yeah, so thanks for that question. And I think this is a very

important point, and Judge Wald started it and you have continued it.

We have to be really very clear about what international law is. International law is not principles that we think would be fine, policy principles that you and I might agree.

International law, if we are serious about international law, and this actually is the definition of international law, are things that nations agree to, to be bound by, by treaty or that is customary internationally, meaning that countries do it so often that everybody does it and they do it by a sense of binding legal obligation.

So two points here, and Judge Wald, I heard you say that while it is true that other countries actually take a broader definition of whether the ICCPR applies extra-territorially, I'm not aware of any country in the world that believes that the ICCPR actually binds them with respect to electronic surveillance, that that right to privacy in Article 17 actually limits

their ability to conduct electronic surveillance of foreign nationals. So that is just not a treaty obligation that countries have accepted, even under the ICCPR.

It might be something that human rights groups wish were the case, but it is not something that governments have accepted, and certainly not something the United States government has accepted.

And then just one more round on the Human Rights Committee. Again, the treaty itself does not say that the decisions of the Human Rights Committee, which is basically a group of academic experts, are binding. Governments who write treaties know how to write language.

For example, the U.N. Charter says that we undertake to comply with rulings of the ICJ. But the human rights monitoring groups, countries have not said that we undertake to comply with their decisions.

And in fact, the senate, and all of you know this, the senate would never agree to cede

responsibility for the future interpretation of a treaty to a group of academic experts. That would take completely out of the hands of the shared understanding between the executive and senate, the interpretation of a treaty.

So you know, the United States, and this is the view of the Obama administration as well, you know, recognizes that other people may not agree on the extraterritorial application of the ICCPR, but you know, no country believes that the ICCPR actually limits electronic surveillance.

MS. COLLINS COOK: So I just wanted to as a follow-up question to Ms. Pitter. Thank you. I know we've aimed a lot of our questions at you.

I think there's a sense within the United States government, a little bit of exasperation, the concern is that our surveillance lacks transparency or that we are somehow outside the mainstream of what other countries are doing.

And I look at 702 in particular and I see something where our legislative branch has specifically said exactly what our executive

branch can do. The executive branch, which is headed by democratically accountable individuals then oversees the execution of that authority, it is subject to the oversight of the judicial branch and it is subject to the oversight of our legislative branch.

So I guess my question is systemically what else could the United States be doing to help build the confidence and trust of other countries?

MS. PITTER: So the oversight so far has all been in secret. I think that's one problem. I mean even the first panel today said they were in the process of declassifying a large number of documents and they were looking at doing that because they recognize the importance of transparency.

The oversight has not, I mean if you look at what happened with 215, even --

MS. COLLINS COOK: I was talking about Section 702, which is the focus of our --

MS. PITTER: We don't know the details of the oversight regarding 702, so the only

information I have about oversight would be regarding 215. And we saw that the judicial oversight in that context, you know, would up, there was an opinion that had an impact on the vast number of communications of Americans that was kept secret from the Americans, so --

MS. COLLINS COOK: Well, let me push back a little bit on this notion that the oversight is not transparent.

So again, we have a statute that tells the world exactly what the executive branch must present to the judiciary, what findings the judiciary must make, what authority judiciary has vis-a-vis that application, and the framework for this surveillance.

We have a public statute that also tells you exactly what the executive branch is obligated to share with Congress. So where's the lack of transparency in that?

MS. PITTER: Well, the judicial oversight for the 702 program is annual. They look at just the procedures. They don't actually

look at the individual targeting requirements. That's done by an NSA analyst at his computer desk.

MS. COLLINS COOK: Actually I think if you were here for the first panel the testimony by the first panel was that that is not in fact the case, that it is an ongoing process of oversight. There are regular reporting requirements, both to the court and to the Congress, so.

MS. PITTER: I was, I did hear the first panel, and I believe he said that those targeting decisions by the analysts are reviewed eventually, but it's not something that's done at the beginning. So the --

MS. COLLINS COOK: So if there's not public review of specific targeting decisions, so this, the United States government saying we would like to collect foreign intelligence information about this specific selector, that's a lack of transparency that is problematic for you?

MS. PITTER: Well, the transparency, even the certifications that the FISC court gets,

there's no, they don't even see the identifiers or the selectors, they just approve the procedures. So you know, that's a problem with the oversight. In terms of --

MR. MEDINE: I'm going to let Ms. Brand pick up since we're at time. So thank you.

MS. BRAND: Okay. I guess maybe this question is directed at John but if anyone wants to jump in, that's fine.

If the ICCPR did have application to the U.S. government surveillance of non-U.S. persons abroad, setting aside the territorial issue for a minute, what does privacy mean in that context?

I have found the lack of a universally accepted definition of privacy very frustrating writ large across everything that we do, and I mean the same issue pertains here. So I guess is there a universally accepted definition of privacy? Is there a definition of privacy that is binding on the U.S. government? If not, how would we find, who would supply such a definition? If

you can sort of help us understand that.

MR. BELLINGER: Yeah, so that's a great question. And that's really the third prong. I mean the reason that the ICCPR doesn't apply is, one, there's the within its territory and subject to its jurisdiction. Then even if it were subject to our jurisdiction, then it has to be within the power and control.

And you know, no one is really going to legitimately argue that, as I think you said earlier, power and control in the view of those who take that interpretation of power and control is someone that you actually physically have in your custody, not electronic surveillance.

And then there's the issue, even if those applied, is something unlawful or arbitrary violation of privacy? And there are not definitions that are universally accepted.

You know, people can argue about these things but for it to be law that a country actually violates, there has to be an agreed definition on privacy and there has to be an

agreed definition on what is arbitrary, and there just are not those definitions.

You know, again, someone can say that someone has an absolute right not to have any country pry into anything that they're doing and that that's a violation of their privacy, but there's not an accepted definition of that.

I mean I could frankly imagine if one were to accept the first part of your premise, which is that it were to apply extra-territorially, and let's also say that it were someone within the U.S. jurisdiction, let's say someone, the United States is actually holding a terrorist in another country and we agreed that the ICCPR applied, we agreed the person was within our power and control, and then we were to do extensive interviews of that person about the person's private life, and then we just publish it willy-nilly, not as part of a criminal proceeding but essentially just as a leak, well, you know, there might be an argument that that might be an arbitrary intervention with that person's right to

privacy.

But I think that's -- there's not a definition of privacy, or of arbitrary, or unlawful that is binding as a matter of international law.

MS. BRAND: Chris or Laura, any thoughts on that question?

MS. PITTER: Would you repeat that question again?

MS. BRAND: Just what does privacy mean in the ICCPR context? Where does the definition come from? How would you find the definition?

MS. PITTER: Well, it guards against unlawful and arbitrary interference with an individual's privacy, so there has to be a respect for correspondence, for example, and a respect for an individual's personal space, and there has to be an ability to have personal space to communicate.

MS. BRAND: Where are you getting that definition?

MS. PITTER: Well, that's, I mean

that's coming from the interpretation of, the right to privacy is connected to freedom of expression, freedom of association. It impacts that. And you know, the right to correspondence comes from that as well. So I mean it's defined in the treaty itself, and --

MS. BRAND: What is the definition? Humor me.

MS. PITTER: I mean --

MS. BRAND: I can look it up, never mind. But it sounds like what you're giving me is sort of your sense of what privacy entails, not a sort of legally defined or legally articulated definition. Chris?

MR. WOLF: So a privacy lawyer's answer goes back to Brandeis and Warren who said the right to privacy is the right to be left alone. But they recognized and I think it's been recognized ever since, that was 1890, that there are exceptions for the good of society, for law and order, for social good.

And that's really where the rubber hits

the road. What are the permissible exceptions for national security surveillance? And you know, that's the discussion that needs to be had globally.

You know, Judge Wald asked what should the U.S. government do? I think it should promote that discussion as a global matter, and at the same time I think it should promote the decoupling of national security surveillance from cross-border data flows for commercial purposes.

The threat to withdraw safe harbor, for example, the declaration that the transatlantic trade and investment partnership shouldn't address data because of what happened with national security surveillance is a non sequitur.

Those issues need to be dealt with between governments, but that shouldn't interfere with cross-border data flows, which have to have privacy protections built-in, no question. But those are not something, that isn't something, the surveillance issue is not something that the companies themselves can really address and

they've done about as much as they can in pushing for transparency, pushing very hard.

MR. MEDINE: Dean, did you want to add something?

MR. GARFIELD: The question was asked earlier about what the appropriate venue is and I would say a reminder that the strategic and economic dialogue didn't exist beyond five years ago, and so this is one issue that's getting left behind in the discussion, the importance of creating a framework and a venue for greater multinational dialogue around the surveillance issue. And I think the PCLOB in its recommendations can have a dramatic effect in this area.

MR. SIEBER: It's clear that we have not an international definition because the countries are too different. However, in the countries and national law, and European law and in other legal bodies these definitions are emerging. And of course they have to develop.

What is sure is that there is a core

area of privacy where we all would agree that privacy is infringed. For example, if you directly do intelligence gathering on the sexual life of somebody who is not a suspect, there's no reason, that's a clear core area infringement of privacy.

Now if you go further, it's becoming of course a difficult, mass surveillance of people against which there is no suspicion would be one aspect where we'd have to investigate.

Another one is to create a complete picture of the private life of somebody going back to his birth, whatever did he do, did he demonstrate in school? So collecting enormous mass of data on one person would be another aspect, just illustrating. There are cases which fall under something like that.

And we should work on this definition and the fact that we do not have something like that would not lead me to the conclusion we shouldn't go in these things.

It's the same with this attitude on

extraterritorial application and things like that. These questions are so new that you cannot find any government's position here. So for me, that's not a valid argument. If you are pioneers on these questions, we cannot say the governments are not yet there.

I agree with you it's a political question on this issue.

One final point where I do not agree what was said is the question with respect to territoriality. If you are collecting data in a foreign country from (inaudible) it's clear that's legal. You are not infringing the foreign territory.

But if you go to a foreign territory and you switch on servers, you download countries -- the electronic pulses, you are changing and you do a function that usually the police does, this is a clear infringement of territoriality.

And you can see this especially in the cyber crime convention where we are fighting about these questions. We have Article 32 B with a big

struggle between the U.S. and Russia, which is bringing down the complete process of the cyber crime convention. We all agree that except these cases mentioned in Article 32 of the cyber crime convention ratified by the U.S., any police activities doing access to foreign countries are of course infringements of privacy. Nobody would claim that this is legal. We could stop the process of the cyber crime convention if your statement would be, all right, like that in this generality.

So I would say that we have to remain -- these surveillance activities do not in any case infringe territoriality but there are many cases, especially looking at the cyber crime convention, our agreements which we have on this committee, we all would say that's a clear infringement of the sovereign territoriality of a country. And it is also undisputed that the protection of territoriality is guaranteed, not only by Article 2 of the U.N. Charter, but also by customary law. It's one of the basic principles

since the Westphalia Peace Accord.

MR. MEDINE: Let's give John a chance to respond.

MR. BELLINGER: I'll be brief. On the second point, again I would say that I don't think any country in the world would say that the Article 2 of the U.N. Charter's protection of the territorial integrity and sovereignty of states would mean that they cannot conduct essentially espionage activities from anywhere. I just don't think that's what the U.N. Charter says.

But more importantly, the first thing you said really goes to the heart of our discussion here, where you said this is an evolving national dialogue about privacy and it is a dialogue that is going on nationally in different countries, and it therefore is going on internationally.

But the question at least that was put to several of us, to me and Laura in particular is, is there a binding international law standard right now? And the answer to that is clearly no.

Germany may have laws inside Germany, given its particular past. Other countries may have particular national laws. Sooner or later countries may get together and agree on things, but right now there is not an international legal standard, either in the ICCPR or anywhere else that limits electronic surveillance from the United States, or again, from any other country.

Other countries would not agree that there's not an international legal standard -- or that there is an international legal standard.

MR. MEDINE: We have time for just a quick round that Jim had requested. Let me just ask just to clarify one point, John, the treaty ICCPR is not self-executing. What does that mean and is there any forum in which enforcement action could take place?

MR. BELLINGER: That means that it would require implementing legislation for it to be, so it's binding as a matter of international law and we have implemented it already and are in compliance with it in certain ways because of laws

that we already had on our books, or might thereby have our Congress pass. But it does not have automatic legal effect merely by the United States becoming party to it.

MR. MEDINE: And is there any forum in the world where we could be held accountable for compliance with the ICCPR?

MR. BELLINGER: The U.N. Human Rights Committee monitors our compliance and comments upon things that we are doing. That's what happened last week when we presented our report. And the United States commented on or responded to these comments, but that's not judicially or legally enforceable.

MR. MEDINE: Thanks. Judge Wald.

MS. WALD: Just a quick comment. Am I not right, John, that not in this context of surveillance, but hasn't England at times relied in some of its judicial decisions on the ICCPR for the, to disallow, I think in dealing with some detainees or asylum people, etcetera?

So my impression was there are courts

who have actually relied upon the ICCPR, not in the surveillance context but in other contexts.

MR. BELLINGER: You and I would have to look at those together. It may have been the European Convention on Human Rights. There has been a fair amount of jurisprudence recently on the extent to which the European Convention on Human Rights creates obligations on British and European forces who actually do have someone within their control of their military outside of Britain, or Germany, or elsewhere.

MS. WALD: Okay. I'll let you off. Very quickly I have one question, quickly, for Mr. Garfield, and that is that the statement that your organization provided to us spoke of the need for meaningful oversight by an independent body in government as to the surveillance programs, including access to collected data.

Just wondered very quickly, who you had in mind, was it the IGs, us, FISA, Congress? Did you have particular independent bodies who would provide the meaningful insight, which included in

your statement oversight of collected, access to the collected data?

MR. GARFIELD: We did not.

MS. WALD: Okay, that's a succinct answer.

MR. MEDINE: Gives you a concise answer.

MR. DEMPSEY: Rather than a question I'll just offer an invitation, which is if any of the witnesses could provide us with guidance on the question I posed, what would be a better way of structuring a foreign intelligence system.

I think at the end of the day any concept of law, any set of rules is going to recognize that different countries are going to have somewhat different structures. So the German structure is robust but different from the United States. The United States believes it has a robust system with different elements than Germany has, etcetera.

Has anybody put together or could anybody put together a list of the elements of a

system and then some sense of how you come up with what is the minimum?

We talked a lot about judicial oversight but Germany does not have. The court reviews the statutory structure but not the individual implementation, does not do individual targeting on the strategic surveillance in Germany. In the U.K. it's all administerial, not judicial.

Secondly, if any further thoughts on how we get from here to there. So several witnesses have said it's an evolving situation. We have new questions, questions which to my view are not answered in the existing documents. Let's just say that it's not answered. They don't apply. No one thought about this. It hasn't been answered. How do we move forward, we, the world, or maybe the U.S. and Europe, which have more shared values than we sometimes admit, how do we move forward in getting that kind of commitment?

And the industry in Garfield's paper is that a global, I think implicitly recognizes we

need global understanding, even if not all of the laws are the same.

So any thoughts that you can offer us. Not right now because we want to move along, but any further follow-up thoughts you could offer us in writing, please, it would be very helpful on both of those points.

MS. COLLINS COOK: I just wanted to thank you all for coming. As I said at the beginning I think it's important to have these discussions. I won't assign homework or request any follow-up, but it's an education process for us, as well as for the American people, particularly on these issues.

So if there is information you think should be a part of the public record, which will remain open, I'm sure David will explain, it is welcomed.

MS. BRAND: I won't take up anymore of your time since we are at the end of our schedule here. But I want to thank all of you for coming. It was very helpful to me, so thank you for taking

the time to prepare and to be here.

MR. MEDINE: Thanks again to all the speakers and the Board staff that made this hearing possible. The Board's activities for today are now complete.

The Board encourages all those who are interested to submit, panelists and members of the public, to submit written comments on this topic at our website of www.regulations.gov. And the deadline for submitting comments is March 28th. All comments submitted will be available for review by the public. A transcript of today's hearing will be posted on PCLOB.gov.

And I will now move to adjourn the hearing. All in favor of adjourning the hearing please say aye.

(Aye)

MR. MEDINE: Upon receiving unanimous consent to adjourn, we will now adjourn. The time is 3:40. Thank you.

(Whereupon, at 3:40 p.m., the hearing was adjourned.)

CERTIFICATION

I, LYNNE LIVINGSTON, A Notary Public of the State of Maryland, Baltimore County, do hereby certify that the proceedings contained herein were recorded by me stenographically; that this transcript is a true record of the proceedings.

I further certify that I am not of counsel to any of the parties, nor in any way interested in the outcome of this action.

As witness my hand and notarial seal this _____ day of _____, 2013.

_____

Lynne Livingston

Notary Public

My commission expires: December 10, 2014

B

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix R

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Follow-up Questions Regarding Section 702 Certifications
June 17, 2011

1. The government's Response to the Court's Briefing Order of May 9, 2011 ("June 1 Submission") states that Internet transactions acquired by NSA in its upstream collection may contain not only multiple discrete communications (some of which are neither to, from, nor about a tasked selector), but also [redacted] June 1 Submission at 25.

a. Please provide some examples of the [redacted] For instance, could such acquisitions include [redacted]

b. What is the likelihood that such [redacted] pertain to persons other than the users of tasked selectors, including persons in the United States or U.S. persons?

2. The June 1 Submission states that "no NSA analyst has yet discovered in NSA's repositories a wholly domestic communication." June 1 Submission at 9.

a. What is meant by "wholly domestic communication" in this statement? Does the term include the discrete communications that might be embedded within acquired transactions?

b. What is the likelihood that an analyst viewing information obtained through a transactional acquisition would have a basis for determining that a discrete communication embedded within the transaction is purely domestic?

3. a. Might the non-targeted portion of a transaction ever be the sole basis for that transaction being responsive to an analyst's query?

b. Upon retrieving information in response to a query, can an analyst readily distinguish that portion of a transaction that contains the targeted selector from other portions of a transaction?

4. a. Please describe the manner in which the government minimizes discrete communications and other information that is contained within acquired Internet transactions but that is neither to, from, nor about the user of a targeted selector.

b. In particular, please explain how the government applies the provisions of NSA's minimization procedures that use the term "communication" to the discrete communications and other non-target information contained within the transactions that are acquired. See, e.g., NSA Minimization Procedures § 2(c) (defining "[c]ommunications of a United States person"); § 2(e) (defining "foreign communication" and "domestic communication[]"), § 3(b)(4) (discussing determination whether a communication is "foreign" or "domestic"), and § 5 (discussing handling of domestic communications).

~~TOP SECRET//COMINT//ORCON,NOFORN~~

c. Would all communications and [redacted] within a transaction be treated the same when the minimization procedures are applied, or would there be different treatment?

5. a. Once NSA has identified a portion of a transaction that does not contain targeted information, is it possible to mask or otherwise minimize the non-target information contained within the transaction?
b. Why is NSA unable to delete and replace, or alter, an original transaction that contains non-target information? See June 1 Submission at 27-28.

6. The government states that an Internet transaction that is acquired "is . . . not divisible into the discrete communications within it even once it resides in an NSA corporate store." June 1 Submission at 22. Please reconcile that statement with the government's acknowledgment that "an analyst would . . . be able to copy a portion of the rendered view of a transaction contained in a NSA corporate store and then paste it into a new record on a different system." Id. at 27 n.25.

7. Please reconcile the government's statement that the "communicants" of to/from communications are "the individual users of particular selectors" (see June 1 Submission at 30) with [redacted] elsewhere in its response to the Court's questions (see, e.g., id. at 6 (discussing application of IP filtering)).

8. What is the factual basis for NSA's assertions that "a United States person would use [redacted] only in a minute percentage of cases" and that "[redacted] See June 1 Submission at 11, 12.

9. What is the factual basis for NSA's suggestion that [redacted] See June 1 Submission at 8 n.9

10. The government repeatedly characterizes as "unintentional" NSA's collection of discrete non-target communications as part of transactional acquisitions, [redacted] Assuming arguendo that such collection can fairly be characterized as unintentional, please explain how 50 U.S.C. § 1806(i) applies to the discrete, wholly domestic communications that might be contained within a particular transaction.

11. Please provide a thorough legal analysis supporting your view that the knowing and intentional acquisition of large volumes of Internet transactions containing discrete communications that are neither to, from, nor about a targeted selector (as well as other information not pertaining to the users of targeted selectors) is merely "incidental" to the authorized purpose of the collection as a whole, and therefore reasonable under the Fourth Amendment.

12. The statute requires the targeting procedures to "be reasonably designed to ensure that any acquisition . . . is limited to targeting persons reasonably believed to be located outside the United States and [to] prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." 50 U.S.C. § 1881a(d)(1). How can procedures that contemplate the knowing acquisition of huge volumes of transactions that will include quantifiable amounts of information relating to non-targets, including information of or about U.S. persons abroad or persons located in the United States, meet this statutory requirement?

13. In its discussion of the Fourth Amendment, the government asserts that "upstream collection" in general is "an essential and irreplaceable means of acquiring valuable foreign intelligence information that promotes the paramount interest of protecting the Nation and conducting its foreign affairs." June 1 Submission at 16.

a. To what extent can the same be said for the acquisition of Internet transactions [redacted] in particular?

b. Is the acquisition of Internet transactions via upstream collection the only source for certain categories of foreign intelligence information? If so, what categories?

c. Please describe with particularity what information NSA would acquire, and what information NSA would not acquire, if NSA were, in comparison to its current collection, to limit its acquisition of Internet communications to: (1) acquisitions conducted with the assistance of [redacted]; and (2) the upstream collection of discrete communications to, from, or about tasked selectors that are [redacted] (id. at 2, n.2).

14. The Fourth Amendment also requires the Court to examine the nature and scope of the intrusion upon protected privacy interests. How can the Court conduct such an assessment if the government itself is unable to describe the nature and scope of the information that is acquired or the degree to which the collection includes information pertaining to U.S. persons or persons located in the United States?

15. In light of the government's emphasis on the limited querying of Section 702 acquisitions that is currently permitted (see June 1 Submission at 23), why is it reasonable and appropriate to broaden the targeting procedures to permit querying using U.S.-person identifiers?

16. The government acknowledges that it previously "did not fully explain all of the means by which . . . communications are acquired through NSA's upstream collection techniques" (June 1 Submission at 2), yet states that the "[Attorney General] and [Director of National Intelligence] have confirmed that their prior authorizations remain valid" (id. at 35). At the time of each previous Certification under Section 702, were the Attorney General and the Director of National Intelligence aware that the acquisitions being approved included Internet "transactions" [redacted]? If so, why was the Court not informed. If not, why are the prior Certifications and collections still valid?

~~SECRET//ORCON,NOFORN~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

2011 JUN 28 PM 4:51

WASHINGTON, D.C.

[redacted]

NOTICE OF FILING OF GOVERNMENT'S RESPONSE
TO THE COURT'S SUPPLEMENTAL QUESTIONS OF JUNE 17, 2011

THE UNITED STATES OF AMERICA, through the undersigned Department of Justice attorney, respectfully submits the attached factual and legal response to the

~~SECRET//ORCON,NOFORN~~

Classified by: ~~Tashina Gauhar, Deputy Assistant Attorney General, NSD, DOJ~~
Reason: 1.4(c)
Declassify on: ~~28 June 2036~~

~~SECRET//ORCON,NOFORN~~

supplemental questions provided by this Court to the Government on June 17, 2011, concerning the above-referenced matters. Given the complex nature of the Court's questions and the Government's responses, the United States is prepared to provide any additional/supplemental information the Court believes would aid it in reviewing these matters. The Government may also seek to supplement and/or modify its response as appropriate during any hearing that the Court may hold in the above-captioned matters. ~~(S//OC,NF)~~

Respectfully submitted,

[redacted]

National Security Division
United States Department of Justice

~~SECRET//ORCON,NOFORN~~

VERIFICATION

I declare under penalty of perjury that the facts set forth in the attached Government's Response to the Court's Supplemental Questions of June 17, 2011, are true and correct based upon my best information, knowledge and belief. Executed pursuant to Title 28, United States Code, § 1746, on this 28th day of June, 2011. ~~(S)~~

[redacted]

Signals Intelligence Directorate Compliance Architect
National Security Agency

~~TOP SECRET//COMINT//ORCON/NOFORN~~

GOVERNMENT'S RESPONSE TO THE COURT'S FOLLOW-UP QUESTIONS OF JUNE 17, 2011

1. The government's Response to the Court's Briefing Order of May 9, 2011 ("June 1 Submission") states that Internet transactions acquired by NSA in its upstream collection may contain not only multiple discrete communications (some of which are neither to, from, nor about a tasked selector), but also [redacted] June 1 Submission at 25.

a. Please provide some examples of the [redacted] For instance, could such acquisitions include [redacted]

b. What is the likelihood that such [redacted] pertain to persons other than the users of tasked selectors, including persons in the United States or U.S. persons?

As was more fully explained in the Government's June 1 Submission, the presence of a tasked selector is required in order for the National Security Agency's (NSA) upstream Internet collection devices to identify and then acquire Internet communications in the form of transactions. *See* June 1 Submission at 1, 24-26. The Court's question in 1.a. further asks whether such transactions could include [redacted]. Personal information, including that of persons other than a user of a tasked selector, could be acquired by NSA in relation to any one or more of these communication services to the extent it is included within a transaction. This, however, is true even with respect to discrete communications to,

[1] [redacted] ~~(S)~~

~~TOP SECRET//COMINT//ORCON/NOFORN~~

Classified by: Tashina Gauhar, Deputy Assistant Attorney General, NSD, DOJ
Reason: 1.4(c)
Declassify on: ~~28~~ June 2036

from, or about a tasked selector, depending on what the communicants chose to include within, [redacted] the communication. [redacted] ~~(TS//SI//NF)~~

Although personal information may be included in a transaction, the manner in which NSA conducts its upstream collection significantly diminishes the likelihood that such information would pertain to U.S. persons or persons in the United States. As discussed more fully in the Government's response to question 14 below, NSA acquires certain transactions because they contain a discrete communication to or from a tasked selector used by a person who, by virtue of the application of NSA's targeting procedures, is a non-United States person reasonably believed to be located outside the United States. NSA acquires transactions that contain a discrete communication about a tasked selector using technical means that are designed to ensure that such acquisition is directed at a person reasonably believed to be located outside the United States. The Court has previously recognized that "the vast majority of persons who are located overseas are non-United States persons and that most of their communications are with other, non-United States persons, who are located overseas." *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, Docket No. 105B(g):07-01, Mem. Op. at 87 (USFISC April 25, 2008) (footnote omitted) (hereinafter "*In re Directives to Yahoo!* Mem. Op."). Thus, it is reasonable to presume that most of the discrete communications that may be within an acquired transaction are between non-United States persons located outside the United States. ~~(TS//SI//OC/NF)~~

2. The June 1 Submission states that "no NSA analyst has yet discovered in NSA's repositories a wholly domestic communication." June 1 Submission at 9.

a. What is meant by "wholly domestic communication" in this statement? Does the term include the discrete communications that might be embedded within acquired transactions?

By "wholly domestic communication" the Government means a communication as to which the sender and all intended recipients are located within the United States. The Government includes within this term any discrete communication within a transaction where the sender and all intended recipients of the discrete communication were located in the United States at the time the communication was acquired. With the previously described limited exception involving [redacted] NSA analysts have yet to identify a wholly domestic communication in any transaction acquired through NSA's upstream collection systems. ~~(TS//SI//NF)~~

b. What is the likelihood that an analyst viewing information obtained through a transactional acquisition would have a basis for determining that a discrete communication embedded within the transaction is purely domestic?

The likelihood that an NSA analyst would recognize that a transaction containing either a discrete communication (e.g., an e-mail message) or multiple discrete communications [redacted] contains a wholly domestic communication depends on a number of factors, including: [redacted] ~~(TS//SI//OC/NF)~~

3.a. Might the non-targeted portion of a transaction ever be the sole basis for that transaction being responsive to an analyst's query?

Yes. All information acquired by NSA as a result of tasking the targeted foreign person's selector -- whether initially determined to be foreign intelligence information to, from, or about that targeted foreign person (or foreign intelligence information concerning other foreign persons or organizations) or incidentally acquired information concerning other currently non-targeted persons -- can be queried by analysts for foreign intelligence information. As a result, it is possible that any portion of a transaction could be the sole basis for that transaction being responsive to an analyst's foreign intelligence query of NSA databases. Such queries (which are subject to review), however, must be formulated by an analyst in accordance with NSA minimization procedures which require that computer selection terms used for scanning, such as telephone numbers, key words or phrases, or other discriminators, be limited to those selection terms reasonably likely to return foreign intelligence information. *See, e.g.,* Amendment 1 to

[2] [redacted] ~~(TS//SI//NF)~~

DNI/AG 702(g) Certification [redacted] Ex. B, filed Aug. 12, 2010, § 3(b)(5) (hereinafter "Current NSA Minimization Procedures").[3] ~~(TS//SI//NF)~~

3.b. Upon retrieving information in response to a query, can an analyst readily distinguish that portion of a transaction that contains the targeted selector from other portions of a transaction?

Yes. The tasked selector that resulted in NSA's acquisition of any particular transaction is discernable by analysts reviewing information in response to a query. The analytic tools used to display an acquired transaction allow NSA analysts to identify the tasked selectors that resulted in the acquisition of the transaction, thereby enabling analysts to determine the portion(s) of the transaction in which that selector appears. In some instances, the analyst may need to review the entirety of the transaction (including the underlying metadata or raw data) to identify where the tasked selector appears, but even in these situations, the tasked selector is included and identifiable. [redacted] ~~(TS//SI//NF)~~

4.a. Please describe the manner in which the government minimizes discrete communications and other information that is contained within acquired Internet transactions but that is neither to, from, nor about the user of a targeted selector.

4.b. In particular, please explain how the government applies the provisions of NSA's minimization procedures that use the term "communication" to the discrete communications and other non-target information contained within the transactions that are acquired. See, e.g., NSA Minimization Procedures § 2(c) (defining "[c]ommunications of a United States person"); § 2(e) (defining "foreign communication" and "domestic communication[]"), § 3(b)(4) (discussing determination whether a communication is "foreign" or "domestic"), and § 5 (discussing handling of domestic communications).

4.c. Would all communications [redacted] within a transaction be treated the same when the minimization procedures are applied, or would there be different treatment?

---

[3] The Government seeks the Court's approval of revised NSA Section 702 minimization procedures that would enable NSA analysts to use United States person identifiers as selection terms if those selection terms are reasonably likely to return foreign intelligence information. *See, e.g.*, DNI/AG 702(g) Certification [redacted], Ex. B, filed Apr. 20, 2011, § 3(b)(5) (hereinafter "Proposed NSA Minimization Procedures"). Under these revised NSA Section 702 minimization procedures, the use of such selection terms must be approved in accordance with NSA procedures designed to ensure that the selection terms are reasonably likely to return foreign intelligence information. *Id.* The Government is still in the process of developing the NSA procedures governing the use of United States person identifiers as selection terms. Until those procedures are completed, NSA analysts will not begin using United States person identifiers as selection terms. ~~(TS//SI//NF)~~

As required by FISA, *see* 50 U.S.C. §§ 1881a(e), 1801(h), and 1821(h), NSA's minimization procedures address the acquisition, retention, and dissemination of non-publicly available information concerning unconsenting United States persons. *See* Current Minimization Procedures, § 1.[4] When NSA acquires an Internet transaction that contains multiple discrete communications, NSA considers each of those communications to be separate "communications" under its minimization procedures. Thus, for example, an NSA analyst would consider each discrete communication within a larger Internet transaction as a separate communication for purposes of determining whether the communication is a foreign or domestic communication under NSA's minimization procedures. *See, e.g.,* Current and Proposed NSA Minimization Procedures, § 2(e). ~~(TS//SI//OC/NF)~~

The manner in which acquisitions are conducted under Section 702 operates to minimize the acquisition of information about United States persons. First, certain transactions are acquired because they contain a discrete communication to or from a tasked selector used by a person who, by virtue of the application of NSA's FISC-approved targeting procedures, is a non-United States person reasonably believed to be located outside the United States. This Court has recognized that "the vast majority of persons who are located overseas are non-United States persons and that most of their communications are with other, non-United States persons, who are located overseas." *In re Directives to Yahoo!* Mem. Op. at 87 (footnote omitted). Accordingly, it is reasonable to presume that most of the discrete communications that may be within the acquired transaction -- even those that are not to or from a tasked selector -- are between non-United States persons located outside the United States. Second, with respect to transactions that contain a discrete communication about a tasked selector, the technical means by which NSA prevents the intentional acquisition of wholly domestic communications are designed to ensure that the acquisition of transactions is directed at persons reasonably believed to be located outside the United States. As a result, these persons reasonably also can be presumed to be non-United States persons, and most of their communications -- including those that are not about a tasked selector -- can be presumed to be with other non-United States persons located outside the United States. *Id.* This combination of targeting non-United States persons located outside the United States and directing acquisitions at persons located outside the United States operates to significantly diminish the amount of information pertaining to United States persons or persons in the United States that NSA acquires through its upstream collection. *See* [redacted] Mem. Op. at 23 (recognizing that "[t]he targeting of communications pursuant to Section 702 is designed in a manner that diminishes the likelihood that U.S. person information will be obtained"). ~~(TS//SI//OC/NF)~~

To be sure, it is possible that a transaction containing multiple discrete communications only one of which is to, from, or about a tasked selector could contain U.S. person information. The acquisition of such information is an unavoidable by-product of the acquisition of the foreign intelligence information (i.e., the communication to, from, or about a tasked selector) within the transaction. Yet it is important to note that, for purposes of the application of NSA's current and proposed minimization procedures, the Government does not consider its acquisition

[4] NSA's proposed minimization procedures currently before the Court address these same issues. *See* Proposed NSA Minimization Procedures § 1. ~~(S)~~

of a discrete communication within a transaction that is not to, from, or about a tasked selector to be "inadvertent." Subsection 3(b)(1) of NSA's current and proposed minimization procedures require inadvertently acquired communications to be destroyed if they are "identified either: as clearly not relevant to the authorized purpose of the acquisition (e.g., the communication does not contain foreign intelligence information); or as not containing evidence of a crime which may not be disseminated under these procedures." Current and Proposed NSA Minimization Procedures, § 3(b)(1). ~~(TS//SI//NF)~~

As described below in the Government's response to question 10, the Government considers a discrete communication that is not to, from, or about a tasked selector within a transaction to be acquired "incidentally," rather than "inadvertently." In the context of minimization, "incidental" and "inadvertent" should not be considered synonymous. Given that the acquisition of the transaction is intentional, and given the Government's knowledge that such transactions may also include information that is not to, from, or about a tasked selector, the acquisition of this additional information is not "inadvertent." By contrast, the additionally acquired information is "incidental" in that it is not the basis for the collection but is rather a necessary yet unavoidable consequence of acquiring foreign communications to, from, or about a tasked selector. *See* [redacted] Mem. Op. at 40 (concluding that the Government's minimization procedures "constitute a safeguard against improper use of information about U.S. persons that is inadvertently *or* incidentally acquired") (emphasis added).[5] Otherwise, subsection 3(b)(1) of NSA's current and proposed minimization procedures would require the destruction of the *entire* transaction -- even the very foreign intelligence information that resulted in the transaction's acquisition in the first place -- if any discrete communication therein contained United States person information and was not to, from, or about a tasked selector. ~~(TS//SI//OC/NF)~~

Such an absurd result simply cannot be squared with Congress's explicit intent that non-pertinent information should be destroyed only if "feasible." *See* H.R. Rep. No. 95-1283, pt. 1, at 56 ("By minimizing retention, the committee intends that information acquired, which is not necessary for obtaining[,] producing, or disseminating foreign intelligence information, be destroyed *where feasible*." (emphasis added)). Congress recognized that in some cases, pertinent and non-pertinent information may be co-mingled in such a way as to make it technologically infeasible to segregate the pertinent information from the non-pertinent information and then

[5] The Government notes that at a single point in its June 1 Submission, it incorrectly described the acquisition of a discrete communication that is not to, from, or about a tasked selector within a transaction to be acquired "inadvertently." *See* June 1 Submission at 13 ("The issue for the Court in light of the above-described nature and scope of NSA's upstream collection is whether, in light of a governmental interest 'of the highest order of magnitude,' NSA's targeting and minimization procedures sufficiently protect the individual privacy interests of United States persons whose communications are inadvertently acquired."). However, the Government otherwise consistently described the acquisition of such communications as "incidental," *see, e.g.*, *id.* at 15 ("NSA's upstream collection may incidentally acquire information concerning United States persons within transactions containing multiple discrete communications, only one of which is to, from, or about a person targeted under Section 702."); *id.* at 19 ("The fact that other, non-pertinent information within the transaction may also be incidentally and unavoidably acquired simply cannot render the acquisition of the transaction unreasonable."); *id.* ("[T]o the extent that United States person information is incidentally acquired in the acquisition of a whole transaction by NSA's upstream collection, such information will be handled in accordance with strict minimization procedures."). ~~(TS//SI//NF)~~

destroy the latter. *See id.* ("The committee recognizes that it may not be feasible to cut and paste files or erase part of tapes where some information is relevant and some is not."). Here, it is not technologically feasible for NSA to extract, post-acquisition, only the discrete communication that is to, from, or about a tasked selector within a transaction. Thus, in order for NSA to retain the foreign intelligence information within a transaction, it must retain the entire transaction, including any incidentally acquired information about U.S. persons or persons in the United States contained therein. ~~(TS//SI//NF)~~

This incidentally acquired information in transactions is subjected to the same restrictions on use and dissemination that govern information obtained through other means pursuant to Section 702 (such as through collection at Internet Service Providers).[6] The Court has previously found these restrictions on use and dissemination in NSA's current minimization procedures to be consistent with the Act and the Fourth Amendment. *See, e.g, In re DNI/AG Certification* [redacted] Mem. Op. at 8-12 (USFISC [redacted] 2010); *In re DNI/AG Certification* [redacted] Mem. Op. at 8-15 (USFISC [redacted] 2009). Of course, the Government seeks the Court's approval of revised NSA Section 702 minimization procedures that would enable NSA analysts to use United States person identifiers as selection terms if those selection terms are reasonably likely to return foreign intelligence information. As discussed in its response to question 14 below, the Government respectfully suggests that these revised NSA minimization procedures are also consistent with the Act and the Fourth Amendment. ~~(TS//SI//OC/NF)~~

In sum, NSA treats each discrete communication contained within a larger Internet transaction as a separate communication for purposes of its minimization procedures. Although it is possible that certain discrete communications containing United States person information will be retained, as described above, they remain subject to the same restrictions on use and dissemination imposed by NSA's minimization procedures. ~~(TS//SI//OC/NF)~~

5.a. Once NSA has identified a portion of a transaction that does not contain targeted information, is it possible to mask or otherwise minimize the non-target information contained within the transaction?

No. The analytic tools used to display the acquired data to NSA analysts do not have a capability to mask information or otherwise minimize the non-target information contained within a transaction. See additional details provided in response to question 6 below. ~~(TS//SI//NF)~~

[6] Moreover, as discussed in response to question 3.b. above, NSA's inability to separate the discrete communications post-acquisition also means that the discrete communications are not displayed in NSA's SC-SSRs as separate communications, but rather clearly retain their connection to the entirety of the original transaction, making it more apparent to NSA analysts the discrete communication's relationship to a tasked selector. ~~(TS//SI//OC/NF)~~

5.b. Why is NSA unable to delete and replace, or alter, an original transaction that contains non-target information? See June 1 Submission at 27-28.

The answer to this question is included in the response to question 6 below. ~~(TS//SI//NF)~~

6. The government states that an Internet transaction that is acquired "is... not divisible into the discrete communications within it even once it resides in an NSA corporate store." June 1 Submission at 22. Please reconcile that statement with the government's acknowledgment that "an analyst would . . . be able to copy a portion of the rendered view of a transaction contained in a NSA corporate store and then paste it into a new record on a different system." Id. at 27 n.25.

As discussed in the example of [redacted] information on pages 27-28 of the June 1 Submission, the data within such transactions is organized in a fashion meant to be displayed using [redacted], which is not necessarily a format in which discrete communications that may be contained within the transaction are distinguishable. In order for NSA to identify and separate a transaction containing multiple communications into those component parts, the transaction would require processing, parsing, and reformatting for those components intended for subsequent retention as separate communications. This is true at the point of acquisition and at any point post-acquisition, including at the point of display to the analyst, whether the intent is to separate out a particular communication from the transaction for the purpose of deleting it, replacing it, masking it, or otherwise altering it. [redacted] ~~(TS//SI//OC/NF)~~

Absent [redacted] capabilities as discussed above, attempts by NSA analysts to delete, replace or otherwise alter (e.g., mask or otherwise minimize the non-target information contained within the transaction) a portion of a transaction intercepted through NSA's upstream collection techniques could similarly corrupt the integrity of the collection, destabilizing -- and potentially rendering unusable -- some or all of the collected transaction, including any particular communication therein for analytic or other purposes. Maintaining the integrity of original transactions is paramount to NSA's retention and dissemination processes. Specifically, NSA has developed and implemented a comprehensive purge process designed to improve the completeness of data purges. The efficacy of this process depends in large measure on NSA's ability to trace data back to the original object (such as a transaction) in a SIGINT Collection - Source Systems of Record (SC-SSR). Maintaining the integrity of original transactions is also important for ensuring quality control of NSA's foreign intelligence analysis of Internet communications, which frequently may contain more than one tasked selector or could be used by more than one analyst, depending on the target, mission, or specific foreign intelligence need to which it pertains. Thus, preserving the integrity of the data is dependent upon the retention of the original transaction in its original form as stored in the SC-SSR. ~~(TS//SI//OC/NF)~~

The government's representation that an Internet transaction that is acquired "is... not divisible into the discrete communications within it even once it resides in an NSA corporate store" was intended to convey that it is not technologically feasible for NSA to create [redacted] processes to divide transactions into discrete communications. Footnote 25 on page 27 of the June 1 Submission refers to the fact that it is possible for individual analysts to copy some of the information from a transaction in NSA corporate stores into a new document or file stored on a separate system, such as a [redacted] *See, e.g.*, DNI/AG 702(g) Certification [redacted] Trans. of Proceedings at 20-21 ([redacted] 2010) (for a discussion of [redacted]). The fact that such a copy or extract can be made, however, does not mean that the underlying transaction can then be altered in the corporate store. For example, if an analyst copied a portion of a transaction from an SC-SSR into a [redacted] and then purged the transaction from the SC-SSR, the data copied into the [redacted] would likewise have to be purged -- even if it contained foreign intelligence information copied from a communication to, from, or about a tasked selector -- because it could no longer be traced back to an object present in an SC-SSR. ~~(TS//SI//OC/NF)~~

7. Please reconcile the government's statement that the "communicants" of to/from communications are "the individual users of particular selectors" (see June 1 Submission at 30) with [redacted] elsewhere in its response to the Court's questions (see, e.g., id. at 6 (discussing application of IP filtering)).

The Government believes its statement that [redacted] in the case of to/from communications is fully consistent with the Government's description of how NSA [redacted] to determine if one end of a to/from communication is outside of the United States. As stated on page 30 of the June 1 Submission, the communicants in to/from communications are the individual users who are the senders and intended recipients of those communications, rather than [redacted] ~~(TS//SI//OC/NF)~~

With respect to IP filtering, however, in many instances it is not possible for NSA to [redacted]. *See* June 1 Submission at 6-7. [redacted] *See, e.g., id.* at 11. ~~(TS//SI//OC/NF)~~

As described in the June 1 Submission, there are scenarios under which NSA could unknowingly and unintentionally acquire a to/from communication in which the sender and all intended recipients are in the United States at the time of acquisition -- for example, if that

communication [redacted][7] In the unlikely event that NSA does unintentionally acquire such a communication, NSA will purge the communication unless its continued retention is authorized by the Attorney General in accordance with 50 U.S.C. § 1806(i). If the communication is itself contained within a transaction that contains other discrete communications, the whole transaction will be purged unless its continued retention is authorized by the Attorney General in accordance with 50 U.S.C. § 1806(i), regardless of whether those other discrete communications are foreign. ~~(TS//SI//OC/NF)~~

8. What is the factual basis for NSA's assertions that "a United States person would [redacted] only in a minute percentage of cases" and that [redacted]? See June 1 Submission at 11, 12.

These factual assertions by NSA are based upon the assessments of NSA Signals Intelligence (SIGINT) personnel, who have been involved in NSA's Section 702 acquisitions since the initiation of that collection, and many of whom have experience [redacted] NSA's factual assertions in the June 1 Submission are also based on its review of a sampling of Section 702-acquired communications, which is described on page 9 of the June 1 Submission. As is more fully discussed in that filing, NSA's review of [redacted] records between these two tests revealed only [redacted] records indicative of a non-targeted user [redacted] in the United States. Further research revealed that these [redacted] records were actually copies of the same transaction, and NSA found no indication that any wholly domestic communications were within this transaction. NSA assesses that the results of these tests are consistent with the assessments made by NSA's SIGINT personnel in the June 1 Submission. ~~(TS//SI//OC//NF)~~

9. What is the factual basis for NSA's suggestion that [redacted]? See June 1 Submission at 8 n.9.

[redacted]

[7] As previously described, it would be very unlikely for [redacted] in which the sender and all intended recipients are located inside the United States. See June 1 Submission at 11. Moreover, with the previously described limited exception [redacted] *see id.* at 6 & n.5, NSA analysts have yet to identify a wholly domestic communication acquired through NSA's upstream collection systems. *See id.* at 9 (noting NSA's experience to date and describing NSA's test samples, stating that the only records possibly indicative of a United States-based user [redacted] did not reveal that any wholly domestic communications had been acquired). ~~(TS//SI//OC/NF)~~

[redacted]

10. The government repeatedly characterizes as "unintentional" NSA's collection of discrete non-target communications as part of transactional acquisitions, [redacted] Assuming arguendo that such collection can fairly be characterized as unintentional, please explain how 50 U.S.C. § 1806(i) applies to the discrete, wholly domestic communications that might be contained within a particular transaction.

Subsection 1806(i) provides that "[i]n circumstances involving the unintentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any communication,[8] under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located in the United States, such contents shall be destroyed upon recognition, unless the Attorney General determines that the contents indicates a threat of death or serious bodily harm to any person." (U)

The Government's June 1 Submission described for the Court that at the time of acquisition, NSA's Section 702 upstream Internet collection devices are generally not capable of distinguishing transactions containing only a single discrete communication to, from, or about a tasked selector from transactions containing multiple discrete communications, not all of which

[8] Subsection 1806(i) originally covered only radio communications, but was amended in 2008 to cover all communications to make it technology neutral. *See* 154 Cong. Rec. S6133 (daily ed. June 25, 2008). (U)

may be to, from, or about a tasked selector at the time of acquisition.[9] *See* June 1 Submission at 7, 27-28. The Government considers the acquisition of communications within a transaction that are not to, from, or about a tasked selector to be incidentally acquired communications. However, the Government does not intend to acquire transactions containing communications that are wholly domestic in nature and in fact has implemented [redacted] means to prevent the acquisition of such transactions. While those [redacted] means could fail (as was the case involving the previously reported [redacted], or be circumvented [redacted] NSA is nevertheless not intending to acquire wholly domestic communications. Thus, in the context of acquiring Internet transactions containing multiple discrete communications, not all of which may be to, from, or about a tasked selector, the Government recognizes that subsection 1806(i) could potentially be implicated to the extent that one of those discrete communications is a communication in which the sender and all intended recipients were located in the United States at the time of acquisition. Accordingly, in the event NSA recognizes a wholly domestic communication which is not to, from, or about a tasked selector which it has unintentionally acquired in the course of conducting its Section 702 upstream Internet collection, NSA would handle the entire transaction in accordance with subsection 1806(i) and either purge it or, if appropriate, seek authorization from the Attorney General to retain it. ~~(TS//SI//OC/NF)~~

NSA's minimization procedures, adopted by the Attorney General in consultation with the Director of National Intelligence, allow the Director of NSA to execute a waiver permitting the retention of wholly domestic communications. *See* Current and Proposed NSA Minimization Procedures, § 5. However, this provision applies to the acquisition of domestic communications when the Government has a reasonable, but mistaken, belief that the target is a non-United States person located outside the United States because NSA is intentionally but mistakenly acquiring such communications.[10] This domestic communications carve-out does not apply to an unintentionally acquired transaction that contains a wholly domestic communication (when recognized as such by NSA) along with other discrete communications, which is not to, from, or about a tasked selector. As described previously, NSA's Section 702 upstream Internet collection devices are generally incapable of distinguishing transactions containing only a single discrete communication to, from, or about a tasked selector from transactions containing multiple discrete communications, not all of which may be to, from, or about a tasked selector at the time of acquisition; moreover, NSA cannot separate transactions containing multiple discrete communications into logical constituent parts post-acquisition. Thus, in the event that NSA's Section 702 upstream Internet collection resulted in the unintentional acquisition of a transaction containing a wholly domestic communication, consistent with subsection 1806(i), NSA would purge the entire transaction, unless the Attorney General has authorized its retention after first

[9] NSA additionally advised the Court that except in certain limited circumstances, NSA cannot separate transactions into logical constituent parts post-acquisition either without rendering the transaction unusable for analytic or other purposes. *See* June 1 Submission at 27 & n.27. ~~(TS//SI//OC/NF)~~

[10] *See* Government's Analysis of Section 1806(i), DNI/AG 702(g) Certification [redacted] Docket No. 702(i)-08-01, filed Aug. 28, 2008; [redacted] Mem. Op. at 25-27. ~~(TS//SI//OC/NF)~~

determining that its contents indicated a threat of death or serious bodily harm to any person.[11] ~~(TS//SI//OC/NF)~~

11. Please provide a thorough legal analysis supporting your view that the knowing and intentional acquisition of large volumes of Internet transactions containing discrete communications that are neither to, from, nor about a targeted selector (as well as other information not pertaining to the users of targeted selectors) is merely "incidental" to the authorized purpose of the collection as a whole, and therefore reasonable under the Fourth Amendment.

Fourth Amendment reasonableness is concerned only with the effect on Fourth Amendment protected interests. Thus, in evaluating reasonableness under the Fourth Amendment, the relevant issue for the Court in considering the acquisition of communications incidental to the purpose of this collection is the extent to which such incidental communications involve United States persons or persons located in the United States. ~~*Cf.* [redacted] Mem. Op. at 37-38 (recognizing that non-U.S. persons outside the United States "are not protected by the Fourth Amendment" (citing *United States v. Verdugo-Urqidez*, 494 U.S. 259, 274-75 (1990)).~~ For the reasons more particularly explained in the Government's responses to question 1 above and question 14 below, most of the communications incidentally acquired pursuant to this collection have no effect on any Fourth Amendment protected interests. The Government acknowledges that it is possible that a transaction containing multiple discrete communications only one of which is to, from, or about a tasked selector could contain information pertaining to United States persons or persons located in the United States. That, however, does not mean that the acquisition of multiple discrete communications is any more likely to result in the acquisition of United States person information than in the collection of single, discrete communications to, from, or about a non-United States person located outside the United States. This is particularly true because the technology NSA uses to prevent the acquisition of wholly domestic communications also acts to limit the acquisition of communications among and between United States persons.[12] ~~(TS//SI//OC/NF)~~

---

[11] See also the Government's response to question 7 above, which explains that there are other scenarios under which NSA could unknowingly and unintentionally acquire a wholly domestic communication. In the unlikely event that NSA does unintentionally acquire such a communication, NSA will purge the communication upon recognition unless its continued retention is authorized by the Attorney General in accordance with subsection 1806(i). If the communication is itself contained within a transaction that contains other discrete communications, the whole transaction will be purged unless its continued retention is authorized by the Attorney General in accordance with subsection 1806(i), regardless of whether those other discrete communications are foreign. ~~(TS//SI//OC/NF)~~

[12] For example, the Court has expressed particular concern regarding the acquisition of [redacted] ~~(TS//SI//OC/NF)~~

Moreover, even with respect to those instances in which U.S. person information is acquired, courts in both the FISA and criminal (Title III) contexts have recognized that the acquisition of communications incidental to the purpose of a collection may be necessary to achieve the goal of a search or surveillance, as well as reasonable under the Fourth Amendment. *See, e.g., In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1015 (Foreign Int. Surv. Ct. Rev. 2008) (hereinafter "*In re Directives*") ("It is settled beyond peradventure that incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful.") (citations omitted)); *United States v. Bin Laden*, 126 F. Supp. 2d 264, 280 (S.D.N.Y. 2000), *aff'd sub nom. In re Terrorist Bombings of U.S. Embassies in East Africa*, 552 F.3d 157 (2d Cir. 2008), *cert. denied sub nom. El-Hage v. United States*, 130 S.Ct. 1050 (2010) ("[I]ncidental interception of a person's conversations during an otherwise lawful [Title III] surveillance is not violative of the Fourth Amendment."). ~~(TS//SI//OC/NF)~~

In cases where NSA acquires Internet transactions that include multiple discrete communications, the Government considers any discrete communications not to, from, or about the tasked selector to be incidentally acquired. Specifically, the Government's purpose in acquiring such a transaction is to acquire the foreign intelligence information likely contained within the discrete communication to, from, or about a tasked selector. However, because it is technologically infeasible for NSA's upstream collection systems to extract only the discrete communication that is to, from, or about a tasked selector, the only way to obtain the foreign intelligence information in that discrete communication is to acquire the entire transaction. Thus, the acquisition of the other discrete communications within the transaction is properly considered "incidental," because it is a necessary but unavoidable consequence of achieving the Government's goal of acquiring the foreign intelligence information contained within the discrete communication to, from, or about a tasked selector. *See* H.R. Rep. No. 95-1283, pt. 1, at 55 (1978) (noting that "in many cases it may not be possible for technical reasons to avoid acquiring all information" when conducting foreign intelligence surveillance); *see also id.* at 56 ("[I]t may not be possible or reasonable to avoid acquiring all conversations."); *cf. United States v. McKinnon*, 721 F.2d 19, 23 (1st Cir. 1983) ("Evidence of crimes other than those authorized in a [Title III] wiretap warrant are intercepted 'incidentally' when they are the by-product of a bona fide investigation of crimes specified in a valid warrant."). ~~(TS//SI//OC/NF)~~

That is not to say, however, that the acquisition of non-pertinent information is reasonable in all cases simply because the collection of that information is "incidental" to the purpose of the search. *United States v. Ulrich*, 228 Fed. Appx. 248, 252 (4th Cir. 2002) (noting that "fishing expeditions" or "a random exploratory search or intrusion" violate the Fourth Amendment) (quotation marks omitted). Here, NSA's acquisition of transactions is conducted in accordance with FISC-approved targeting procedures reasonably designed to ensure that the acquisitions are directed "toward communications that are likely to yield the foreign intelligence information sought, and thereby afford a degree of particularity that is reasonable under the Fourth Amendment." [redacted] Mem. Op. at 39-40 (footnote omitted). The fact that such transactions may contain non-pertinent information -- even in significant amounts -- does not by itself render the acquisition of those transactions unreasonable under the Fourth Amendment. *See Scott v. United States*, 436 U.S. 128, 140 (1978) (recognizing that "there are surely cases,

such as the one at bar [involving a Title III wiretap], where the percentage of nonpertinent calls is relatively high and yet their interception was still reasonable"); *Abraham v. County of Greenville*, 237 F.3d 386, 391 (4th Cir. 2001) ("[I]ncidental overhearing is endemic to surveillance."); *United States v. Doolittle*, 507 F.2d 1368, 1372 (5th Cir. 1975) ("There is no question that some irrelevant and personal portions of gambling conversations were intercepted or that certain nonpertinent conversations were intercepted. But this is inherent in the type of interception authorized by Title III, and we do not view the simple inclusion of such conversations, without more, as vitiating an otherwise valid wiretap.")[13]; *see also, e.g., Board of Educ. v. Earls*, 536 U.S. 822, 837 (2002) ("[T]his Court has repeatedly stated that reasonableness under the Fourth Amendment does not require employing the least intrusive means, because the logic of such elaborate less-restrictive-alternative arguments could raise insuperable barriers to the exercise of virtually all search-and-seizure powers.") (internal quotations marks omitted)). ~~(TS//SI//OC/NF)~~

As such, the incidental collection at issue here is reasonable under the Fourth Amendment because it is a necessary and unavoidable by-product of NSA's effort to obtain the foreign intelligence information contained within a discrete communication that is a part of a larger transaction which could contain non-pertinent communications. *See United States v. Wuagneux*, 683 F.2d 1343, 1352-53 (11th Cir. 1982) (observing that "a search may be as extensive as reasonably required to locate the items described in the warrant," and on that basis concluding that it was "reasonable for the agents [executing the search] to remove intact files, books, and folders when a particular document within the file was identified as falling within the scope of the warrant"); *United States v. Beusch*, 596 F.2d 871, 876-77 (9th Cir. 1979) (rejecting argument that "pages in a single volume of written material must be separated by searchers so that only those pages which actually contain the evidence sought may be seized"). Moreover, as described in the response below, NSA takes the steps it can to ensure that it conducts its Section 702 upstream collection in a manner that minimizes the intrusion into the personal privacy of United States persons. ~~(TS//SI//OC/NF)~~

12. The statute requires the targeting procedures to "be reasonably designed to ensure that any acquisition . . . is limited to targeting persons reasonably believed to be located outside the United States and [to] prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." 50 U.S.C. § 1881a(d)(1). How can procedures that contemplate the knowing acquisition of huge volumes of transactions that will include quantifiable amounts of information relating to non-targets, including information of or about U.S. persons abroad or persons located in the United States, meet this statutory requirement?

[13] These cases upholding the Fourth Amendment reasonableness of Title III surveillances that resulted in the acquisition of significant amounts of nonpertinent communications are particularly noteworthy given that Title Iain's requirement to minimize the acquisition of such communications is considerably stricter than FISA's. *See* H.R. Rep. 95-1283, pt. 1, at 56 ("It is recognized that given the nature of intelligence gathering, minimizing acquisition should not be strict as under [Title III] with respect to law enforcement surveillances."). ~~(TS//SI//NF)~~

For the reasons more particularly discussed in its response to question 1.b.ii. in the June 1 Submission, which took into account the means by which communications to, from, or about a tasked selector are acquired through NSA's upstream Internet collection techniques, the Government respectfully submits that NSA's targeting procedures are reasonably designed to ensure that an authorized acquisition is limited to targeting persons reasonably believed to be located outside the United States, and to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located within the United States. *See* June 1 Submission at 3-12, 20-24. As discussed in the Government's June 1 Submission, for acquisition of both to/from communications and abouts communications, the person being "targeted" is the user of the tasked selector, who, by operation of the targeting procedures, is a non-United States person reasonably believed to be located outside the United States. *See* June 1 Submission at 3-4. This remains true for all Section 702 upstream acquisitions, including the acquisition of transactions containing several discrete communications, only one of which may be to, from, or about the user of a tasked selector. ~~(TS//SI//NF)~~

Specifically, the sole reason a transaction is selected for acquisition is that it contains the presence of a tasked selector used by a person who has been targeted in accordance with NSA's targeting procedures.[14] Indeed, at the time a transaction is acquired, NSA cannot always know whether the transaction includes other data or information representing communications that are not to, from, or about the target, let alone always have knowledge of the parties to those communications. *Cf.* [redacted] Mem. Op. at 18-19 (noting that with respect to abouts communications, "the government may have no knowledge of [the parties to a communication] prior to acquisition"). It therefore cannot be said that the acquisition of a transaction containing multiple discrete communications results in the intentional targeting of any of the parties to those communications other than the user of the tasked selector. *Cf. Bin Laden*, 126 F. Supp. 2d at 281 (acknowledging that in light of *United States v. Verdugo-Urquidez*, 494 U.S. 259, 265 (1990), and Title III "incidental interception" case law, overseas surveillance of a United States person terrorism suspect would have posed no Fourth Amendment problem "if the Government had not been aware of [his] identity or of his complicity in the [terrorism] enterprise"). The fact that a transaction acquired pursuant to the targeting procedures may also contain communications to, from, or about persons other than the user of the tasked selector does not mean those persons are likewise being targeted by that acquisition. *Cf.* H.R. Rep. No. 95-1283, pt. 1, at 50 (explaining, with regard to electronic surveillance as defined by 50 U.S.C. § 1801(f)(1), that "[t]he term 'intentionally targeting' includes the deliberate use of surveillance techniques which can monitor numerous channels of communication among numerous parties, where the techniques are designed to select out from among those communications the communications to which a particular U.S. person located in the United States is a party, and where the communications are

[14] [redacted] ~~(TS//SI//NF)~~

selected either by name or by other information which would identify the particular person and would select out his communications"). Rather, as discussed in the response to question 11 above, the acquisition of such non-pertinent communications is incidental to the purpose of the collection as a whole and therefore reasonable under the Fourth Amendment. ~~(TS//SI//NF)~~

Similarly, to the extent that one of the discrete non-pertinent communications within an acquired transaction is a communication in which the sender and all intended recipients were located in the United States at the time of acquisition, the acquisition of this wholly domestic communication would be incidental and, as discussed in response to question 10 above, unintentional. NSA's targeting procedures require that, in conducting upstream collection of abouts communications, NSA either employ "an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas" or '[redacted]' *E.g.*, Amendment 1 to DNI/AG 702(g) Certification [redacted] Ex. A, filed [redacted] 2010, at 1-2; *see also* [redacted] Mem. Op. at 19. The Court has previously found that these [redacted] means were "reasonably designed to prevent the intentional acquisition of communications as to which all parties are in the United States," while recognizing that it is "theoretically possible that a wholly domestic communication could be acquired as a result of the [redacted] Mem. Op. at 20 & n.17. As discussed in the June 1 Submission, apart from one exception involving [redacted] NSA analysts have yet to identify a wholly domestic communication acquired through NSA's upstream collection systems. *See* June 1 Submission at 8-9. Accordingly, the Government continues to believe that NSA's [redacted] means for preventing the acquisition of wholly domestic communications remain efficacious, and that the theoretical scenarios in which NSA would acquire a wholly domestic communication do not prevent the Court from continuing to find that NSA's targeting procedures are reasonably designed to prevent the intentional acquisition of communications as to which the sender and all intended recipients are known at the time of acquisition to be in the United States. ~~(TS//SI//OC/NF)~~

To the extent that NSA does unintentionally acquire and then recognize such a wholly domestic communication within an acquired transaction, as described in response to question 10 above, NSA would be required to purge the entire transaction, unless the Attorney General determined "that the contents indicate[d] a threat of death or serious bodily harm to any person." ~~(TS//SI//OC/NF)~~

13. In its discussion of the Fourth Amendment, the government asserts that "upstream collection" in general is "an essential and irreplaceable means of acquiring valuable foreign intelligence information that promotes the paramount interest of protecting the Nation and conducting its foreign affairs." June 1 Submission at 16.

a. To what extent can the same be said for the acquisition of Internet transactions [redacted] in particular?

b. Is the acquisition of Internet transactions via upstream collection the only source for certain categories of foreign intelligence information? If so, what categories?

c. Please describe with particularity what information NSA would acquire, and what information NSA would not acquire, if NSA were, in comparison to its current collection, to limit its acquisition of Internet communications to: (1) acquisitions conducted with the assistance of [redacted]; and (2) the upstream collection of discrete communications to, from, or about tasked selectors that are [redacted] (id. at 2, n.2).

The Government's assertion that upstream collection is "an essential and irreplaceable means of acquiring valuable foreign intelligence information that promotes the paramount interest of protecting the Nation and conducting its foreign affairs" is equally applicable to its acquisition of Internet transactions. This is true because the Government's acquisition of Internet transactions is not a subset of its upstream collection of Internet communications. Instead, acquisition of Internet transactions is the technical means by which all upstream collection of Internet communications accounts are acquired. ~~(TS//SI//NF)~~

Section 702 upstream collection of Internet communications provides NSA with certain types of information (further described below) which are extremely valuable to its national security mission. Disseminated end product reports derived from this collection have proven to be of critical value to high-level customers, including the White House, State Department, Joint Chiefs of Staff, the National Counterproliferation Center, Central Intelligence Agency (CIA), Defense Intelligence Agency, Federal Bureau of Investigation (FBI), and others. In addition,

[redacted] ~~(TS//SI//NF)~~

[redacted] ~~(TS//SI//NF)~~

Section 702 upstream collection offers unique opportunities to detect target information, including but not limited to the following examples:

[redacted]

[redacted] ~~(TS//SI//NF)~~

[redacted] As such, and as the Court has recognized, NSA's upstream collection is "*uniquely capable* of acquiring certain types of targeted communications containing valuable foreign intelligence information." *In re DNI/AG Certification* [redacted] Mem. Op. at 25-26 (USFISC [redacted] 2009) (emphasis added; internal citations omitted). ~~(TS//SI//NF)~~

Additionally, NSA's Section 702 upstream collection would not acquire many of the above categories of communications, and thus the foreign intelligence contained within these communications, if NSA's upstream collection were limited to acquisition solely of discrete communications to, from, or about tasked selectors that are [redacted] referenced in footnote 2 on page 2 of the June 1 Submission. Currently, [redacted] ~~(TS//SI//NF)~~

15 [redacted]
(TS//SI//NF)

[redacted]

~~(TS//SI//NF)~~

[redacted] ~~(TS//SI//NF)~~

The Court's question asks for "categories of foreign intelligence information" that can be obtained exclusively through NSA's acquisition of Internet transactions via upstream collection. This is a difficult question to answer, as types of foreign intelligence may be conveyed through a variety of communication means. For example, [redacted] as described above, it is entirely possible that this communication may only be acquired through NSA's Section 702 upstream collection of communications other than those [redacted] ~~(TS//SI//NF)~~

In an effort to fully answer the Court's question, however, the Government respectfully submits the following examples of instances where NSA has obtained substantial foreign intelligence information from Section 702 upstream collection. The examples detail only a few

[redacted]

~~(TS//SI//NF)~~

of the many instances in which Section 702 upstream collection has provided such substantial foreign intelligence. In many of these examples, Section 702 upstream collection provided important leads that led to [redacted]. Although all forms of Section 702 upstream collection have proved to be of critical importance to the NSA's national security mission, the examples below involve the acquisition by Section 702 upstream collection of communications other than [redacted]
~~(TS//SI//NF)~~

[redacted] ~~(S)~~

[redacted]

~~(TS//SI//NF)~~

[redacted] (S)

[redacted]

[redacted]

[redacted] ~~(TS//SI//NF)~~

[redacted] ~~(U//FOUO)~~

[redacted]

14. The Fourth Amendment also requires the Court to examine the nature and scope of the intrusion upon protected privacy interests. How can the Court conduct such an assessment if the government itself is unable to describe the nature and scope of the information that is acquired or the degree to which the collection includes information pertaining to U.S. persons or persons located in the United States?

Although, as discussed above, it is difficult for the Government to fully describe to the Court every possible type of information that may be contained within a transaction acquired through NSA's upstream collection, the Government respectfully suggests that the Court can nonetheless assess whether NSA's upstream collection of such transactions is reasonable under the Fourth Amendment. ~~(TS//SI//OC/NF)~~

First, the Supreme Court has recognized that an appreciation of all of the possible ways a search can intrude upon interests protected by the Fourth Amendment is not an indispensable component of assessing the reasonableness of the search. *See Dalia v. United States*, 441 U.S. 238, 257 (1979) ("Often in executing a warrant the police may find it necessary to interfere with privacy rights not explicitly considered by the judge who issued the warrant."); *cf. Payton v. New York*, 445 U.S. 573, 601-02 (1980) (recognizing that "for Fourth Amendment purposes, an arrest warrant founded on probable cause implicitly carries with it the limited authority to enter a dwelling in which the suspect lives when there is reason to believe the suspect is within," even though "an arrest warrant requirement may afford less [privacy] protection than a search warrant requirement"). Thus, the Government respectfully suggests that the Court can assess the Fourth Amendment reasonableness of NSA's upstream collection even if the Government cannot fully describe every possible type of information that collection may acquire. ~~(TS//SI//OC/NF)~~

Moreover, while it may be difficult for the Government to describe the full scope of the types of information that may be acquired by NSA's upstream collection, it is nevertheless possible to ascertain the degree to which that information would pertain to United States persons or persons located in the United States. For the reasons discussed below, the Government does not believe that information about United States persons or persons located in the United States would be acquired through NSA's upstream collection of transactions to a greater degree, in relative terms, than other types of communications acquired under Section 702. ~~(TS//SI//OC/NF)~~

First, certain transactions are acquired because they contain a discrete communication to or from a tasked selector used by a person who, by virtue of the application of NSA's FISC-approved targeting procedures, is a non-United States person reasonably believed to be located outside the United States. This Court has recognized that "the vast majority of persons who are located overseas are non-United States persons and that most of their communications are with other, non-United States persons, who are located overseas." *In re Directives to Yahoo!* Mem. Op. at 87 (footnote omitted). Accordingly, it is reasonable to presume that most of the discrete communications that may be within the acquired transaction are between non-United States persons located outside the United States. Second, with respect to transactions that contain a discrete communication about a tasked selector, the technical means by which NSA prevents the intentional acquisition of wholly domestic communications is to ensure that the acquisition of transactions is directed at persons reasonably believed to be located outside the United States. Again, these individuals reasonably can be presumed to be non-United States persons, and most of their communications can be presumed to be with other non-United States persons located outside the United States. *Id.* This combination of targeting non-United States persons located outside the United States and directing acquisitions at persons located outside the United States operates to significantly diminish the likelihood that information pertaining to United States persons or persons in the United States will be acquired. ~~(TS//SI//OC/NF)~~

To be sure, it is possible that a transaction containing multiple discrete communications only one of which is to, from, or about a tasked selector could contain information pertaining to United States persons or persons in the United States. That, however, does not by itself mean that the volume of such information in transactions will be greater than in the collection of other types of communications that have previously been discussed and approved. [redacted] ~~(TS//SI//OC/NF)~~

Moreover, the fact that within an acquired transaction there may be multiple discrete communications containing information pertaining to United States persons or persons in the United States cannot by itself render the acquisition of that transaction unreasonable under the Fourth Amendment. As discussed above, the acquisition of such information is incidental to the purpose of the transaction's acquisition -- the acquisition of the discrete communication(s) to,

from, or about a tasked selector within the transaction. *See In re Directives*, 551 F.3d at 1015 ("It is settled beyond peradventure that incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful.") (citations omitted)). ~~(TS//SI//OC/NF)~~

In any event, any information pertaining to a United States person or person located in the United States present in a transaction containing multiple discrete communications would be handled under the NSA minimization procedures in the exact same manner as if that information appeared in a discrete communication to, from, or about a tasked selector. For example, the use and dissemination of United States person information acquired from a [redacted] would be subject to the same restrictions as United States person information acquired from [redacted] ~~(TS//SI//OC/NF)~~

15. In light of the government's emphasis on the limited querying of Section 702 acquisitions that is currently permitted (see June 1 Submission at 23), why is it reasonable and appropriate to broaden the targeting procedures to permit querying using U.S.-person identifiers?

Although NSA's current minimization procedures prohibit the use of United States person names or identifiers to retrieve any Section 702-acquired communications in NSA systems, *see* Current NSA Minimization Procedures, § 3(b)(5), the statute requires no such limitation. Rather, it is reasonable and appropriate for the Court to approve the Government's proposal to enable NSA analysts to use United States person identifiers as selection terms because the request is consistent with the statutorily required minimization procedures. *See* Proposed NSA Minimization Procedures § 3(b)(5) (providing, in pertinent part, that "[c]omputer selection terms used for scanning, such as telephone numbers, key words or phrases, or other discriminators, *will be limited to those selection terms reasonably likely to return foreign intelligence information*. Any United States person identifiers used as terms to identify and select communications must be approved in accordance with NSA procedures.") (emphasis added). ~~(TS//SI//OC/NF)~~

Minimization procedures must be designed to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly availably information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information. 50 U.S.C. § 1801(h)(1). Where, as here, "it may not be possible for technical reasons to avoid acquiring all information," Congress has recognized that minimization procedures "must emphasize the minimization of retention and dissemination." H.R. Rep. No. 95-1283, pt. 1, at 55. Congress also acknowledged that "a significant degree of latitude be given in counterintelligence and counterterrorism cases" with respect to retention and dissemination of information. *Id.* at 59. In light of such latitude, "rigorous and strict controls" should -- and will -- be placed on the retrieval of United States person information and "its dissemination or use for purposes other than counterintelligence or counterterrorism." *Id.* ~~(TS//SI//OC/NF)~~

With respect to acquisition, the Government's proposal to use United States person identifiers as selection terms does not broaden the scope of what the Government can acquire under the certifications. Because, for the reasons detailed above, it is not possible "to avoid acquiring" the incidentally obtained information, the focus will be on the retention and dissemination provisions of the procedures. *Id.* at 55. As a general matter, NSA's minimization procedures contain detailed provisions regarding the retention and dissemination of United States person information that the Court has previously approved. *See, e.g.* [redacted] Mem. Op. at 21-32, 40-41. In addition, the Government's proposal provides that United States person identifiers may only be used "in accordance with NSA procedures" governing the circumstances under which U.S. person information can be queried. Although the Government is still developing such procedures, and NSA analysts will not begin using United States identifiers as selection terms until they are completed, the Government will ensure that the procedures contain "rigorous and strict controls" for the retrieval and dissemination of United States person information to ensure that only selection terms likely to produce foreign intelligence information are retrieved, and dissemination is limited to counterintelligence and counterterrorism purposes. Moreover, the Government's proposed changes to NSA's minimization procedures require that NSA maintain records of all United States person identifiers approved for use as selection terms and that NSD and ODNI conduct oversight of NSA's activities. *See* Proposed NSA Minimization Procedures § 3(b)(5). ~~(TS//SI//OC/NF)~~

16. The government acknowledges that it previously "did not fully explain all of the means by which . . . communications are acquired through NSA's upstream collection techniques" (June 1 Submission at 2), yet states that the "[Attorney General] and [Director of National Intelligence] have confirmed that their prior authorizations remain valid" (id. at 35). At the time of each previous Certification under Section 702, were the Attorney General and the Director of National Intelligence aware that the acquisitions being approved included Internet "transactions" [redacted]? If so, why was the Court not informed? If not, why are the prior Certifications and collections still valid?

The Government acknowledges that its prior representations to the Court -- and to the Attorney General and Director of National Intelligence -- regarding the steps NSA must take in order to acquire single, discrete communications to, from, or about a tasked selector did not fully explain all of the means by which such communications are acquired through NSA's upstream Internet collection techniques. *See* June 1 Submission at 2. That said, for the reasons described in the answer to question 5 in the June 1 Submission, both the prior Certifications and collection remain valid. *See* June 1 Submission at 31-38. ~~(TS//SI//OC/NF)~~

The Certifications executed by the AG and DNI and submitted to the Court for approval were based on an understanding that Section 702 collection would, at a minimum, acquire discrete communications that are to, from, or about a tasked selector. As described in detail previously, due to certain technological limitations, in general the only way that NSA can acquire certain Internet communications upstream that are to, from, or about a tasked selector is by acquiring an Internet transaction which may include a single, discrete communication to, from, or about a tasked selector (e.g., an e-mail message) or may include several discrete

communications, only one of which may be to, from, or about a tasked selector.[17] *See* June 1 Submission at 27-28. In this respect, the acquisition is comparable to the Government's seizure of a video, book, or intact file that contains a single photo, page, or document that a search warrant authorizes the Government to seize. *See, e.g., United States v. Rogers*, 521 F.3d 5, 10 (1st Cir. 2008) (concluding that a videotape is a "plausible repository of a photo" and that therefore a warrant authorizing seizure of "photos" allowed the seizure and review of two videotapes, even though warrant did not include videotapes); *Wuagneux*, 683 F.2d at 1353 (holding that it was "reasonable for the agents to remove intact files, books and folders when a particular document within the file was identified as falling within the scope of the warrant."); *United States v. Christine*, 687 F. 2d 749, 760 (3d Cir. 1982) (*en banc*) (emphasizing that "no tenet of the Fourth Amendment prohibits a search merely because it cannot be performed with surgical precision. Nor does the Fourth Amendment prohibit seizure of an item, such as a single ledger, merely because it happens to contain other information not covered by the scope of the warrant."); *United States v. Beusch*, 596 F.2d 871, 876-77 (9th Cir. 1979) (rejecting argument that "pages in a single volume of written material must be separated by searchers so that only those pages which actually contain the evidence may be seized"). None of these cases even hint that the warrant is somehow invalid because the magistrate did not know in advance that the search or seizure of authorized documents or photos would also encompass the search or seizure of additional, intermingled documents or photos, even in cases where such documents could have been physically separated from the larger files or books in which they were contained. Rather, it is well-established that warrants need not state with specificity the precise manner of execution, and, so long as it is reasonable, a search or seizure will be upheld even if conducted in a manner that invades privacy in a manner not considered at the time the warrant was issued. *See United States v. Grubbs*, 547 U.S. 90, 98 (2006) ("Nothing in the language of the Constitution or in this Court's decisions interpreting that language suggests that, in addition to the [requirements set forth in the text], search warrants also must include a specification of the precise manner in which they are to be executed.") (citation omitted); *Dalia,* 441 U.S. at 259 ("Often in executing a warrant the police may find it necessary to interfere with privacy rights not explicitly considered by the judge who issued the warrant."). ~~(TS//SI//OC/NF)~~

Moreover, having considered the additional information that is being presented to this Court, the AG and DNI have confirmed that the collection fully complies with the statutory requirements of Section 702, as well as the Fourth Amendment, and that therefore the prior Certifications and collection remain valid. *See* June 1 Submission at 35. ~~(TS//SI//OC/NF)~~

As discussed previously, transactions are only acquired if they contain at least one discrete communication to, from, or about a tasked selector. Each tasked selector has undergone review, prior to tasking, to ensure that the user is a non-United States person reasonably believed to be outside the United States. Moreover, with respect to "abouts communications," the targeting procedures are also reasonably designed to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known to be located in the

[17] [redacted] ~~(TS//SI//OC/NF)~~

United States at the time of acquisition. *See id.* at 3-12, 28-30. Just as the Government's acquisition of an entire book based on the fact that a single page falls within the scope of the warrant does not call into question the warrant's specificity, the incidental acquisition of additional communications that are not to, from, or about the tasked selector does not negate the validity of the targeting procedures that are relied on to acquire a particular transaction. ~~(TS//SI//OC/NF)~~

Moreover, the AG and DNI have confirmed that the additional information regarding incidentally acquired communications does not alter the validity of their prior Certifications. *See id.* at 35. As discussed in detail previously, the minimization and targeting procedures fully comport with all of the statutory requirements, including the requirement that the targeting procedures are reasonably designed to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located within the United States, *see id.* at 3-12, 20-24; and the procedures and guidelines are consistent with the requirements of the Fourth Amendment, *see id.* at 13-24. ~~(TS//SI//OC/NF)~~

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix S

This document was also filed as ECF No. 168-30 and can be found in this Joint Appendix at JA3193.

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix T

~~TOP SECRET//SI//NOFORN//20320108~~

EXHIBIT A

PROCEDURES USED BY THE NATIONAL SECURITY AGENCY FOR TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES TO ACQUIRE FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED

~~(S)~~ These procedures address: (I) the manner in which the National Security Agency/Central Security Service (NSA) will determine that a person targeted under section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended (FISA or "the Act"), is a non-United States person reasonably believed to be located outside the United States ("foreignness determination"); (II) the post-targeting analysis done by NSA to ensure that the targeting of such person does not intentionally target a person known at the time of acquisition to be located in the United States and does not result in the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States; (III) the documentation of NSA's foreignness determination; (IV) compliance and oversight; and (V) departures from these procedures.

I. (S) DETERMINATION OF WHETHER THE ACQUISITION TARGETS NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES

~~(S)~~ NSA determines whether a person is a non-United States person reasonably believed to be outside the United States in light of the totality of the circumstances based on the information available with respect to that person, including [redacted]

~~(S)~~ NSA analysts examine the following three categories of information, as appropriate under the circumstances, to make the above determination: (1) they examine the lead information they have received regarding the potential target or the facility that has generated interest in conducting surveillance [redacted]; (2) they conduct research [redacted] to determine whether NSA knows the location of the person, or knows information that would provide evidence concerning that location; and (3) they conduct [redacted] to determine or verify information about the person's location. NSA may use information from any one or a combination of these categories of information in evaluating the totality of the circumstances to determine that the potential target is located outside the United States.

~~Derived From: NSA/CSSM 1-52~~
~~Dated: 20070108~~
~~Declassify On: 20320108~~

~~TOP SECRET//SI//NOFORN//20320108~~

~~(TS//SI)~~ In addition, in those cases where NSA seeks to acquire communications about the target that are not to or from the target, NSA will either employ an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas, or [redacted] In either event, NSA will direct surveillance at a party to the communication reasonably believed to be outside the United States.

~~(S)~~ Lead Information

~~(S)~~ When NSA proposes to direct surveillance at a target, it does so because NSA has already learned something about the target or the facility or facilities the target uses to communicate. Accordingly, NSA will examine the lead information to determine what it reveals about the physical location of the target, including [redacted]

~~(S)~~ The following are examples of the types of lead information that NSA may examine:

[redacted]

~~(S)~~ Information NSA Has About the Target's Location and/or Facility or Facilities Used by the Target

~~(S)~~ NSA may also review information in its databases, including repositories of information collected by NSA and by other intelligence agencies, [redacted], to determine if the person's location, or information providing evidence about the person's location, is already known. The NSA databases that would be used for this purpose contain information culled from signals intelligence, human intelligence, law enforcement information, and other sources. For example, [redacted]

[redacted]

~~(S)~~ NSA [redacted]

~~(S)~~ NSA may also [redacted] to assist it in making determinations concerning the location of the person at whom NSA intends to direct surveillance. For example, NSA may examine the following types of information:

[redacted]

~~(S)~~ **Assessment of the Non-United States Person Status of the Target**

~~(S)~~ In many cases, the information that NSA examines in order to determine whether a target is reasonably believed to be located outside the United States may also bear upon the non-United States person status of that target. For example, [redacted] Similarly, information contained in NSA databases, including repositories of information collected by NSA and by other intelligence agencies, may indicate that the target is a non-United States person.

~~(S)~~ Furthermore, in order to prevent the inadvertent targeting of a United States person, NSA [redacted]

[redacted]

(~~S~~) [redacted]

(~~S~~) Assessment of the Foreign Intelligence Purpose of the Targeting

(~~S~~) In assessing whether the target possesses, is expected to receive, and/or is likely to communicate foreign intelligence information concerning a foreign power or foreign territory, NSA considers, among other things, the following factors:

a. With respect to telephone communications:

- [redacted]

[1] (~~TS//SI//NF~~) [redacted]

- [redacted]

b. With respect to Internet communications:

- [redacted]

[redacted]

- [redacted]

II. ~~(S)~~ POST-TARGETING ANALYSIS BY NSA

~~(S//SI)~~ After a person has been targeted for acquisition by NSA, NSA will conduct post-targeting analysis. Such analysis is designed to detect those occasions when a person who when targeted was reasonably believed to be located outside the United States has since entered the United States, and will enable NSA to take steps to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States, or the intentional targeting of a person who is inside the United States. Such analysis may include:

a) ~~(S)~~ For telephone numbers:

- [redacted]
- NSA analysts may analyze content for indications that a foreign target has entered or intends to enter the United States. Such content analysis will be conducted according to analytic and intelligence requirements and priorities.

b) ~~(S)~~ For electronic communications [redacted]

- Routinely checking all electronic communications [redacted] tasked pursuant to these procedures [redacted] to determine if an electronic communications [redacted] was accessed from inside the United States. [redacted]

[redacted]

[redacted]

- [redacted]

- NSA analysts may analyze content for indications that a target has entered or intends to enter the United States. Such content analysis will be conducted according to analytic and intelligence requirements and priorities.[2]

~~(S)~~ If NSA determines that a target has entered the United States, it will follow the procedures set forth in section IV of this document, including the termination of the acquisition from the target without delay. [redacted].

~~(S)~~ NSA analysts will also analyze content for indications that a target is a United States person.[3] Such content analysis will be conducted according to analytic and intelligence requirements and priorities. If NSA determines that a target who at the time of targeting was believed to be a non-United States person is believed to be a United States person, it will follow the procedures set forth in section IV of this document, including the termination of the acquisition from the target without delay.

III. (S) DOCUMENTATION

~~(S)~~ Analysts who request tasking will document in the tasking database a citation or citations to the information that led them to reasonably believe that a targeted person is located outside the

---

[2] ~~(S)~~ [redacted]

[3] ~~(S)~~ [redacted]

United States. Before tasking is approved, the database entry for that tasking will be reviewed in order to verify that the database entry contains the necessary citations.

~~(S)~~ A citation is a reference that identifies the source of the information, [redacted] The citation will enable those responsible for conducting oversight to locate and review the information that led NSA analysts to conclude that a target is reasonably believed to be located outside the United States.

~~(S)~~ Analysts also will identify the foreign power or foreign territory about which they expect to obtain foreign intelligence information pursuant to the proposed targeting.

IV. ~~(S)~~ OVERSIGHT AND COMPLIANCE

~~(S)~~ NSA will implement a compliance program, and will conduct ongoing oversight, with respect to its exercise of the authority under section 702 of the Act, including the associated targeting and minimization procedures adopted in accordance with section 702. NSA will develop and deliver training regarding the applicable procedures to ensure intelligence personnel responsible for approving the targeting of persons under these procedures, as well as analysts with access to the acquired foreign intelligence information understand their responsibilities and the procedures that apply to this acquisition. NSA has established processes for ensuring that raw traffic is labeled and stored only in authorized repositories, and is accessible only to those who have had the proper training. NSA will conduct ongoing oversight activities and will make any necessary reports, including those relating to incidents of noncompliance, to the NSA Inspector General and OGC, in accordance with its NSA charter. NSA will also ensure that necessary corrective actions are taken to address any identified deficiencies. To that end, NSA will conduct periodic spot checks of targeting decisions and intelligence disseminations to ensure compliance with established procedures, and conduct periodic spot checks of queries in data repositories.

~~(S)~~ The Department of Justice (DOJ) and the Office of the Director of National Intelligence (ODNI) will conduct oversight of NSA's exercise of the authority under section 702 of the Act, which will include periodic reviews by DOJ and ODNI personnel to evaluate the implementation of the procedures. Such reviews will occur approximately once every two months.

~~(S)~~ NSA will report to DOJ, to the ODNI Office of General Counsel, and to the ODNI Civil Liberties Protection Officer any incidents of noncompliance with these procedures by NSA personnel that result in the intentional targeting of a person reasonably believed to be located in the United States, the intentional targeting of a United States person, or the intentional acquisition of any communication in which the sender and all intended recipients are known at the time of acquisition to be located within the United States. NSA will provide such reports within five business days of learning of the incident. Any information acquired by intentionally targeting a United States person or a person not reasonably believed to be outside the United States at the time of such targeting will be purged from NSA databases.

~~(S)~~ NSA will report to DOJ through the Deputy Assistant Attorney General in the National Security Division with responsibility for intelligence operations and oversight, to the ODNI

Office of General Counsel, and to the ODNI Civil Liberties Protection Officer, any incidents of noncompliance (including overcollection) by any electronic communication service provider to whom the Attorney General and Director of National Intelligence issued a directive under section 702. Such report will be made within five business days after determining that the electronic communication service provider has not complied or does not intend to comply with a directive.

~~(S)~~ In the event that NSA concludes that a person is reasonably believed to be located outside the United States and after targeting this person learns that the person is inside the United States, or if NSA concludes that a person who at the time of targeting was believed to be a non-United States person is believed to be a United States person, it will take the following steps:

1) Terminate the acquisition without delay and determine whether to seek a Court order under another section of the Act. If NSA inadvertently acquires a communication sent to or from the target while the target is or was located inside the United States, including any communication where the sender and all intended recipients are reasonably believed to be located inside the United States at the time of acquisition, such communication will be treated in accordance with the applicable minimization procedures.

2) Report the incident to DOJ through the Deputy Assistant Attorney General in the National Security Division with responsibility for intelligence operations and oversight, to the ODNI Office of General Counsel, and to the ODNI Civil Liberties Protection Officer within five business days.

V. ~~(S)~~ DEPARTURE FROM PROCEDURES

~~(S)~~ If, in order to protect against an immediate threat to the national security, NSA determines that it must take action, on a temporary basis, in apparent departure from these procedures and that it is not feasible to obtain a timely modification of these procedures from the Attorney General and Director of National Intelligence, NSA may take such action and will report that activity promptly to DOJ through the Deputy Assistant Attorney General in the National Security Division with responsibility for intelligence operations and oversight, to the ODNI Office of General Counsel, and to the ODNI Civil Liberties Protection Officer. Under such circumstances, the Government will continue to adhere to all of the statutory limitations set forth in subsection 702(b) of the Act.

7/24/14
Date

Eric H. Holder, Jr.
Attorney General of the United States

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix U

FOREIGN INTELLIGENCE SURVEILLANCE COURT

IN RE: DNI/AG 702(g) .
CERTIFICATION [redacted] . [redacted], 2008
~~(S)~~ .
. . . . . Washington, D.C.

TRANSCRIPT OF PROCEEDINGS
BEFORE THE HONORABLE MARY A. McLAUGHLIN
UNITED STATES FISC JUDGE

APPEARANCES:

Department of Justice: (b)(6); (b)(7)(C) [redacted]
MATTHEW OLSEN

National Security Agency: [redacted]

P R O C E E D I N G S

THE COURT: Good morning again, everyone, and we are on the record. Well, thank you all for coming. I really appreciate it. Before I swear in the nonlawyers who will be speaking, let me just get everybody to introduce themselves, at least those who may be participating in this, and that perhaps I guess could be everybody. Is this [redacted]

[redacted] to my far left and [redacted] And then go ahead, sir.

[redacted]: [redacted] (b)(6); (b)(7)(C), National Security Division.

THE COURT: All right.

(b)(6); (b)(7)(C): (b)(6); (b)(7)(C) from the National Security [redacted]

MR. OLSEN: Matt Olsen from National Security [redacted]

THE COURT: Then we're with (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C) FBI.

(b)(6); (b)(7)(C), FBI.

(b)(6); (b)(7)(C), FBI Office of General [redacted]

[redacted] from NSA General Counsel's [redacted]

THE COURT: And especially those in the back, please speak up so the court reporter can hear you and the little mic can pick up. So that was [redacted] and this is?

[redacted]: I'm [redacted] the FISA technical lead from Oversight and Compliance at NSA.

THE COURT: Thank you. Yes, ma'am.

(b)(6) I'm here on behalf of the Director of National Intelligence, Office of General Counsel.

[redacted]: [redacted] from NSA/OGC.

[redacted]: [redacted] from NSA.

[redacted] (b)(6): I'm (b)(6) from the Office of General Counsel for CIA.

THE COURT: Very good. And why don't we have our staff introduce themselves as well.

(b)(6) [redacted]

THE COURT: All right. Thank you.

Now I would like to swear in the nonlawyers who may be speaking today. Whoever that consists of, do you want to rise? I'll do it all at one time. All right.

(The witnesses are sworn.)

THE COURT: Well, let me state for the record why we're here, although I think we all do know why we're here.

The purpose of today's hearing is for the Court to receive additional information and/or clarification with respect to its judicial review under section 702(i) of the FISA Amendments Act of 2008.

The Court, of course, did receive from the government on August 5, 2008, an ex parte submission entitled "Government's Ex Parte Submission of [redacted] and Related Procedures and Requests for an Order Approving Such Certification and Procedures."

At that point, the Court reviewed the submission, as the staff did, and after that the staff met with certain members of the government and relayed my questions and their questions to the government. We then received yesterday, August 26, a document entitled "Government's Preliminary Responses to Certain Questions Posed By the Court."

That was very helpful to get that, and I know you must have had to work hard to put it together on such short notice. So I appreciate it, and it was very helpful.

What I'd like to do today is go over some questions that I still have. I think your written response answered -- the questions that you did deal with I think were answered completely, and I probably won't be doing too much with them. I may just want to confirm a couple of things.

Then I have some additional questions that I think probably you're prepared for because the staff raised them, but I didn't

see them in your responses. Okay?

All right. Let me just start with, again, this first couple things I'm doing relates to what you filed yesterday, and again it's just to sort of pinpoint a couple of things on page 5 of yesterday's submission where you were responding to my question concerning [redacted]

In particular, I raise the issue of some concern about the phrase [redacted]

And you did a lengthy response to that, and I appreciated it, and I just want to sort of confirm and hone in on the fact that it is going to be a situation where you're all going to try -- they're going to try to figure out whether this person is a U.S. person. That was the only issue I had, was what's the due diligence that will go on.

And especially I'm impressed with the second bullet point where you said, [redacted] And then you go on and elaborate.

So I just want to get a confirmation that this is not a situation where, [redacted]

[redacted] I mean, it's after due diligence and analysis [redacted] That is correct, Your Honor. As you know, the statute requires us to have a reasonable belief that a target is located outside the United States. The targeting procedures are designed to ensure that NSA analyzes information that gives rise to that reasonable belief. So it is the targeting procedures that imposes the due diligence requirement on the NSA in that respect.

THE COURT: Okay. That's fine. And I think that answers my question.

My next question with respect to what you had given us is on No. 6, page 7, and it's the discussion of the post targeting analysis done by NSA in the targeting procedures, and my question was the procedure said that that [redacted] and I sort of asked that that be fleshed out a little bit, and you all did, and the first two points I understand.

I wasn't too sure, though, what the meaning of the third bullet point was. I mean, I understand the words, but I'm wondering if someone could flesh that out for me a little. It says, "In all cases, analysts remain responsible for following their target's location and for the validity of continued acquisition of information regarding the target."

[redacted] It's my understanding -- and, [redacted] correct me if I'm wrong -- NSA analysts track particular targets. So it is the analyst who determines the extent to which they need to rely on content analysis to determine a target's location as opposed to something more [redacted]. But it is ultimately the analyst's responsibility for maintaining a reasonable belief that that target is located outside the United States.

And I don't know if you'd like to elaborate on that, [redacted]

[redacted] That's correct, and every selector that goes into an NSA [redacted] database has an analyst's name identified with that so we know who bears the ultimate responsibility, and we have processes set up in place to ensure they're doing their work.

THE COURT: Could you just do a minute or two on the processes?

[redacted]: Yes, ma'am. How far back should I start?

THE COURT: I don't know what that means, "how far back," but just hone in on the fact that they're responsible for following their target's locations; in other words, for following it and the validity of the continued acquisition. So having made the initial foreignness determination, how do you go about making sure they are remaining responsible?

[redacted] The first thing they would do, they would [redacted]

[redacted] And if NSA did intercept information, the first thing they would be responsible for would be to review the content of that information to ensure they got the right target and that it was providing foreign intelligence.

Once they do that, they're going to periodically check that depending on [redacted] the analyst has to ensure that they've reviewed that target and that it is meeting a foreign intelligence purpose.

THE COURT: Okay. Any of the staff have any questions on that topic before I move away from it?

All right. Now, this next one relates to an issue that came up at the December '07 hearing before Judge Kotelly on the Protect America Act, and it relates to oversight reviews.

Obviously, the targeting procedures that we're talking about now, at least with respect to the location of potential targets, are similar to what was reviewed by Judge Kotelly and requires oversight reviews by personnel of Justice and the Office of the Director of National Intelligence.

I read the transcript of the hearing before Judge Kotelly, and she took a lot of testimony concerning the oversight up to that point. Can somebody fill me in on where we are today on

that? Has the methodology that's been used by the reviewers changed at all? Could somebody summarize the results of those reviews?

(b)(6); (b)(7)(C) The methodology has been changed. It's been refined. Back in December, because of the volume of selectors and because we hadn't worked through an exact process in how we would conduct our oversight, we weren't in a position to be able to review every single tasking decision that the NSA had made.

We would do it on a sampling basis. Sometimes we randomly picked certain days and we would look at tasking decisions for those days, or if we had a range of selectors that had been tasked, we would randomly select the sources of information upon which the foreignness determinations for those particular selectors were based.

Since then, we've refined our process such that we're actually able to at the very least receive all of the documentation concerning every single tasking decision that NSA has made. Typically, they're sent to us in electronic format.

So we receive those, we print them off, and we review them to make sure that all of the documentation that the targeting procedures require is present, that being a notation about the foreign intelligence purpose of the collection and the source of the information upon which the foreignness determination for that particular selector was based.

~~As~~ we've gone on and we've refined our methodology and we've had back-and-forth with NSA over how we can improve their performance with respect to filling out particular fields in the sheets, as a result of that back-and-forth, we've actually had to review less and less sources because NSA is relying more and more on [redacted] we don't necessarily need to review per se.

I mean, the most common source of information that NSA relies upon is [redacted]

[redacted] selector is used by a [redacted] So therefore, we don't necessarily need to delve into too much more behind that foreignness determination [redacted]

[redacted]

So I guess in a nutshell, we've been able to do basically

more oversight because our oversight over time has become more efficient.

THE COURT: And how about -- and maybe you've in one sense maybe answered this in part, but what's the result of the reviews been? What are the problems you're seeing at this point?

(b)(6); (b)(7)(C) I would say the most common problem -- and "common" is a relative term here, because the volume of selectors is huge, and the number of problems that we're actually seeing is relatively small. As I've said, as we've engaged in oversight and engaged NSA in discussions on how they can improve the sheets and tasking determinations and things of that nature, the number of problems that we've seen have diminished over time.

I would say the most common problem is to the extent that a tasking determination is based on a wide range of information, there may be a problem with how the source of that information is cited, whether it be somebody just inadvertently mistyped [redacted] or inadvertently left out a [redacted] a key piece of information that was part of the broader range of circumstances upon which NSA made its foreignness determination.

So it's more the little technical things that we've been seeing problems with on a very small scale, and as I've said, it's diminished over time.

THE COURT: I think before Judge Kotelly you identified about [redacted] cases where it appeared that a targeted person was in the U.S., and again, I don't even think I know what time frame that was for, but in any event, can you do anything like that now? I mean, since that hearing in December of '07.

(b)(6); (b)(7)(C) Since that time, that number captured a number of different types of incidents that were reported to us. There are incidents where there's true noncompliance with the targeting procedures that results in basically an improper tasking, whether it be because the person was actually located in the United States or the person was a U.S. person and we did not have 2.5 authority to target that person.

That number also captured instances where NSA had a reasonable belief that the person was located outside the United States at the time of targeting but since that time has roamed into the United States, what we call a "roaming incident."

A third type of incident that that number captured is what we would call a tasking error where NSA would run a particular facility through its targeting procedures but in the act of actually targeting that, by keying in the account or phone number into the tasking tool, there was a typo or something of that nature.

At the time of the hearing, we hadn't fully determined which incidents fell necessarily into which category. Since

that time, we've had an opportunity to do that. And for incidents that were reported to us through May 9 of this year, [redacted] incidents involved instances where a target was targeted improperly under the targeting procedures.

We had [redacted] incidents -- one of the things that NSA is required to do when they identify somebody who has roamed into the States is to notify us of that within 72 hours of making that determination.

We had [redacted] instances where a person had roamed into the States but the NSA did not meet that 72-hour reporting requirement. But in all of those [redacted] cases, the tasking itself was reasonable; it's just that they failed to comply with the reporting requirement.

We're tracking a number of other incidents, but with respect to those incidents, we're pretty much in the same posture that we were back in December: They've been reported to us; we don't have all the facts with respect to those incidents yet in order to be able to categorize them and say, okay, this is a true noncompliance incident, this is just a roaming incident, or this is just a tasking error.

THE COURT: Now, the [redacted] situations where you hadn't been notified within 72 hours, you picked it up in a review much later, or how did it come -- did they report it in 72 hours plus 10, or was it picked up when you went over and --

[redacted] No. They actually reported those to us.

THE COURT: Okay.

[redacted] It was just for a variety of reasons they could not comply with the 72 hours. Sometimes it's just because a final determination can take a little while simply to the extent that the information is somewhat ambiguous. I think NSA errs on the side of caution and probably sets the date of that determination sooner rather than later such that the 72-hour reporting requirement is triggered basically at the first instance or first indication as opposed to when a final determination is made.

Again, we've sort of refined the reporting requirement and have explained to NSA basically when that 72-hour reporting requirement kicks in such that we've, again, seen less and less of these incidents as time has gone on.

THE COURT: So you've taken steps to make sure that NSA, their people understand at least your view of the 72 hours in order to cut down on the situations where things aren't reported.

[redacted] Yes. That's one of the most, I think, valuable aspects of the oversight visits. It's not just to, you know, we sit there and we review and go over things with NSA, but then we sort of have -- at the end, we sort of have a roundup where we all talk about issues that have been identified and ways that we can either fix problems or correct things. And I think we've won the fruits of that, as I said, because the

number of incidents we've seen has been diminishing over time.

THE COURT: Okay. Now, what do you foresee under the FISA Amendments Act? Do you foresee the same procedures for your oversight being implemented? Are you planning on different procedures? What are your thoughts?

(b)(6); (b)(7)(C) I can't say for certain. I would anticipate that things would not change, simply because in my view they've been working very well. As I've said, we've seen improvement, I think, just the whole process as we've refined it over the last year. I think where we are right now is probably -- we're in a good spot with respect to oversight, in my view.

THE COURT: All right. Well, what about the non-U.S. person status, which of course is new under the FISA Amendments Act? Are you going to be changing anything in terms of focusing on that?

(b)(6); (b)(7)(C) We already sort of do with respect to -- the U.S. person status is so intertwined with the location of the target [redacted] to the extent that in the past NSA would actually affirmatively identify targeted U.S. persons to us on the sheets, because one of the additional fields that they put in the sheets is basically a blurb, an explanation and a description of the target.

Clearly, we're not allowed to target U.S. persons anymore, so I don't anticipate seeing any such descriptions on the

sheets. But again, since the status of the person, the determination of how that is made is so intertwined with the same information upon which NSA relies to make a foreignness determination, that it would be hard for us not to identify such information as we're conducting the reviews.

THE COURT: Has there been -- and maybe you've said this, but is there thought to be or are you planning to or have you already sat down with people or issued things so that they can now focus on the fact that we've got the non-U.S. person status, which is also something they need to be focusing on?

[redacted] I don't think we've had formal discussions about it. Again, this wasn't an issue that has cropped up out of nowhere where we sort of had to still deal with this issue in the context of the Protect America Act, because under the certifications, we were not allowed to target U.S. persons unless we had 2.5 authority.

THE COURT: Okay.

[redacted] So we always had this affirmative -- although it was not affirmatively stated in the targeting procedures, there was an implicit requirement to ensure that we're not inadvertently or intentionally targeting U.S. persons in the absence of such authority.

So the types of checks that we're doing now build upon checks that we were doing previously in order to satisfy that requirement or limitation.

THE COURT: (b)(6) did you want to follow up on that at all? I know you guys were here last time. Anything?

(b)(6); (b)(7)(C): I don't think I have anything.

THE COURT: Okay. Thank you on that.

My next issue has to do with departures from procedures, if I can phrase it that way. Let me find out where we're going.

Here we are. I know that -- at least I believe the staff talked with you about this before this hearing, and it's page 10 of the targeting procedures. Let me just get them out.

"If, in order to protect against immediate threat to the national security, the NSA determines that it must take action, on a temporary basis, in apparent departure from these procedures," and I know that -- again, was it at the hearing perhaps? I'm not remembering whether it was at the hearing or not. In any event, I know in the past there has been a representation of the situations that you contemplate coming within this. I don't think you dealt with that in your response from yesterday.

(b)(6); (b)(7)(C): No, we didn't.

THE COURT: Okay. Could you just confirm for us -- I know you've already had discussions with staff, but tell me what you expect to be contemplated by this provision.

(b)(6); (b)(7)(C): First, I think the circumstances under which this provision would be triggered would be very extreme

circumstances: an imminent terrorist attack or a terrorist attack that has occurred or something of equal significance. With respect to the types of departures, I mean, in all cases we will continue to adhere to the limitations set forth in the statute.

We are anticipating that the types of departures would be on a more technical level such as perhaps because NSA personnel are devoted to addressing or countering this terrorist threat, they may not be able to devote the resources necessarily for us to conduct an oversight review within the allotted 60 days.

THE COURT: Has this been used? Has the PAA provision ever been used?

(b)(6); (b)(7)(C) [redacted] We've never invoked it.

THE COURT: Never invoked. Okay. Can you give me a little more meat on the bones on what you would contemplate?

[redacted]. [redacted] I think the other situation we thought of is an emergency, as (b)(6); (b)(7)(C) describes, and our actual system for recording things is down. So technically we can't get to the system where we'd record this. We'd still make a note of what we've done, so we would comply substantially with what's required, we wouldn't want the issue to arise and prevent us from doing what we need to do, are we complying in every detail.

So that's the kind of thing that I think we contemplate

that it could be used in, and again, my own expectation is it will never be used, but we did provide for it in the unlikely event.

THE COURT: Okay. All right. Let's talk for a little bit about these *about* communications.

What I would find very helpful -- can someone just briefly and with not a lot of technical but some technical aspects talk to me about how communications are acquired? Are they acquired in a different way than the *to-or-from* communications? I mean, as I understand it, you're not acquiring them from Internet service providers, like (b)(1); (b)(3); (b)(7)(E) [redacted]

[redacted]: Judge, if I may, I'm going to let [redacted] come to the table because he's one of the people who can explain this.

THE COURT: Oh, wonderful. Come on up, sir. This is [redacted]

[redacted] Yes, typically for *about* communications, right now we do not acquire them from Internet service providers [redacted]

So what happens there is you pick up things like two unknown communicants to us and the *to-from* talking about one of

our targeted selectors. That's a very useful case to us because

(b)(1); (b)(3); (b)(7)(E)

That's one example.

Another example is (b)(1); (b)(3); (b)(7)(E)

(b)(1); (b)(3); (b)(7)(E)

In other arenas as well, (b)(1); (b)(3); (b)(7)(E)

same kind of thing. We maybe find (b)(1); (b)(3); (b)(7)(E) of a known target that provides a unique insight into that foreign intel need.

And another example, just to flesh these out, a bit more is we would have a target who (b)(1); (b)(3); (b)(7)(E)

(b)(1); (b)(3); (b)(7)(E)

(b)(1); (b)(3); (b)(7)(E)

(b)(1); (b)(3); (b)(7)(E)

THE COURT: (b)(1); (b)(3); (b)(7)(E)

(b)(1); (b)(3); (b)(7)(E) How do you do it?

(b)(1); (b)(3); (b)(7)(E)

(b)(1); (b)(3); (b)(7)(E)

THE COURT: Yeah.

-- that then ensures (b)(1); (b)(3); (b)(7)(E)

(b)(1); (b)(3); (b)(7)(E)

(b)(1); (b)(3); (b)(7)(E)

(b)(1); (b)(3); (b)(7)(E)

THE COURT: Okay. Can we talk for a minute -- obviously, the issue for the Court and for the government, as you came up with all these procedures, is the reasonableness

standard, and the Court is looking at that as well as, obviously, compliance with the Fourth Amendment, which in itself is a reasonableness standard, I guess, as well.

Do the *abouts* present a different issue in terms of the reasonableness, do you think? Let me just expand a little bit on that and have some response to it.

What percentage of the acquisitions are *abouts*, as opposed to *to* and *from*? Is an *about* acquisition more or less likely to pick up communications that otherwise you wouldn't be allowed to pick up for whatever reason? Do they present harder issues for reasonableness?

Somebody want to start discussing that with me? Have you thought about that?

[redacted] As far as the percentage number, we don't have a number for that, because as I mentioned earlier, when we [redacted] we find *to's* and *froms* and [redacted] so we don't categorize those separately to be able to count those communication as *abouts*.

So we don't have any numbers. I can tell you as far as usefulness, they're very useful, and we see them routinely, but I don't have a number for you on that.

THE COURT: And in terms of the usefulness, their importance to what you're trying to accomplish, talk to me a little bit about that. As important as a *to* or *from*, less important? What role do they play in what you're doing?

[redacted] They're very useful in [redacted]

[redacted]

So, for example, in the [redacted] (b)(1); (b)(3); (b)(7)(E) [redacted] (b)(1); (b)(3); (b)(7)(E)

(b)(1); (b)(3); (b)(7)(E)

[redacted]

[redacted]

THE COURT: Now, you're saying in your response, still on the *abouts*, "the operation of the Internet protocol address filters or [redacted] prevents the intentional acquisition of communications about the target as to which the senders and all intended recipients are known at the time of acquisition to be located in the U.S."

[redacted] What about the U.S. person status, how that is more difficult to account for or to --

(b)(6); (b)(7)(C) [redacted] Well, first of all, it's our position that the target of an *abouts* communication is still the user of the targeted selector. It's not the sender or recipient of the e-mail or other communication that contains the targeted selector. I mean, that's where the foreign intelligence interests lie, in the user of the targeted selector.

To the extent that the IP filters and [redacted] ensure that at least one end of the communication is outside the United States, more often than not, I would suspect both ends of the communication are outside the United States. We're collecting *abouts* of purely transient communications such that it's less likely that there's U.S. persons involved or U.S.-person information involved.

But even to the extent that one of the communicants was a U.S. person or was located in the United States, to the extent that there's U.S.-person information in the *abouts* communication, that information will be subject to the minimization procedures.

THE COURT: Okay. Anything from staff on the *abouts*? I'm going to talk some more about the filter issue but from a different perspective. Anybody?

[redacted] (b)(6) Judge, I think I do have a question.

THE COURT: Yes. Go ahead, Phil.

[redacted] (b)(6) When you describe how [redacted] these *about* communications, you described it in a way -- well, you said that [redacted] acquiring the *to-or-from* communications [redacted], if you wanted to for whatever reason, would it be technically feasible to -- in the same manner [redacted] would it be technically feasible to acquire only communications that are to or from the selector account and not those communications that otherwise contain a reference or name of a selector account?

[redacted] It is technically feasible. The problem with doing so is if you end up discarding a number of communications that are truly *to-froms* that you should be able to collect but [redacted]

[redacted]

So by trying to limit us to say no *abouts*, then we end up cutting out those kind of communications as well, truly *to-froms*. So it would be -- we're not surgical enough to take that out of the equation without impacting our ability to do *to-froms* effectively.

[redacted] (b)(6) Okay.

[redacted] Judge, may I offer --

THE COURT: Sure. This is [redacted] right?

[redacted] -- as to the reasonableness. I think you asked the question about reasonableness we haven't addressed. But one of the things the way we have this structured, we think it is akin to -- not exactly the same, but akin to finding a connection between a targeted e-mail address and a person outside the United States.

And for that communication only, we think it's reasonable to make that newly discovered person -- to acquire his communications. There's no automated tasking of that newly discovered person that takes place. Nothing happens as a matter of course. We only collect that single communication, and then

we assess it as to whether we want to make a new target there of the person overseas. But it's important, I think, to understand there's no follow-on automated, *now we found a new person, a new person, a new person*, and those are not automatically added to our task mode.

So it's a limited look with our target, the user of the e-mail address continuing to be our target, [redacted]

[redacted]

THE COURT: Yes. I'm glad you brought that up, [redacted] because what I understand, and I think you've just said it, is that when you're picking up the *about*, you're also getting information on the *to* and *from*. But if the *to* or *from* is now a person of interest, but if it's a U.S. person, for example, or something, you couldn't continue to just pick up that person, directed at the person, but then you'd have to come into court with an application or do whatever else. But you're not automatically then following that person.

[redacted] That's correct.

THE COURT: Now, on the IP -- this is getting to minimization, but because it relates to the filters, let's talk about it. And this is on page 5 of your written response from yesterday. The NSA minimization procedures, you're stating, "contain a provision for allowing retention of information

because of limitations on NSA's ability to filter communications." My question I had was is the filter discussed in targeting the same filtering. I just wanted to understand that, and apparently it is.

But talk to me a little bit, because there seemed to be some tension there. [redacted]

[redacted]

(b)(6); (b)(7)(C) I think the inclusion of that provision in the minimization procedures was intended to be prophylactic in the event that the filters don't necessarily work, and NSA has represented that it's been their experience with the filters and [redacted] that they have not captured purely domestic communications with respect to the *abouts*.

But to the extent that [redacted]

[redacted]

this provision basically captures instances where the filters may not work in every instance.

THE COURT: You did respond to this, but I guess maybe just a little bit more on how limited are they. I mean, what are the limitation of these filters?

[redacted] Limitations really come down to -- the

filter is basically [redacted]

[redacted]

[redacted]

THE COURT: (b)(6)

(b)(6) Thank you, Judge.

[redacted]

[redacted]

THE COURT: Okay.

(b)(6) [redacted] With one other question. For example, with the filters, [redacted]

[redacted]

(b)(6) [redacted]

[redacted]

(b)(6) [redacted]:

MR. (b)(6) [redacted]

(b)(6) [redacted]:

[redacted]

MR. (b)(6) [redacted]

[redacted]

(b)(6) [redacted]

[redacted]

MR. (b)(6) [redacted]

[redacted]

THE COURT: Okay. Again, going on or continuing with minimization procedures, let me see where I am here. Just a couple of things that I think the staff confirmed with you prior to the hearing when they raised various issues. And it wasn't in your memo from yesterday, so I'll just raise it here. But as I understand it, (b)(1); (b)(3); (b)(7)(E) [redacted]

(b)(6); (b)(7)(C) That's correct.

THE COURT: Okay. And on page 1, I guess it was, of (b)(1); (b)(3); (b)(7)(E) [redacted]

[redacted] (b)(6); (b)(7)(C) Yes.

THE COURT: All right. And then I wanted to go to 3(b)(1) of the minimization procedures, a paragraph I will tell you that I had some struggles with, but now I think I understand it.

(b)(6) [redacted] This will be the NSA minimizations --

THE COURT: I'm sorry, NSA.

All right. Now, first of all, as I understand it, I thought there was a "not" missing, and there was.

(b)(6); (b)(7)(C) [redacted] There is.

THE COURT: Okay, that's fine. I kept reading and thinking I was missing something, and it took me awhile. But let me just say to you what I understand this paragraph to mean, and then tell me if it -- that "NSA shall destroy inadvertently acquired U.S.-persons communications once they are identified as both clearly not relevant to the authorized purpose of the acquisition and not containing evidence of a crime." And also "inadvertently acquired U.S.-person communications includes these electronic communications acquired because of limitations of the ability to filter." That was the filter issue.

That's what will happen, and the time limit is a maximum of five years.

(b)(6); (b)(7) [redacted]: Correct.

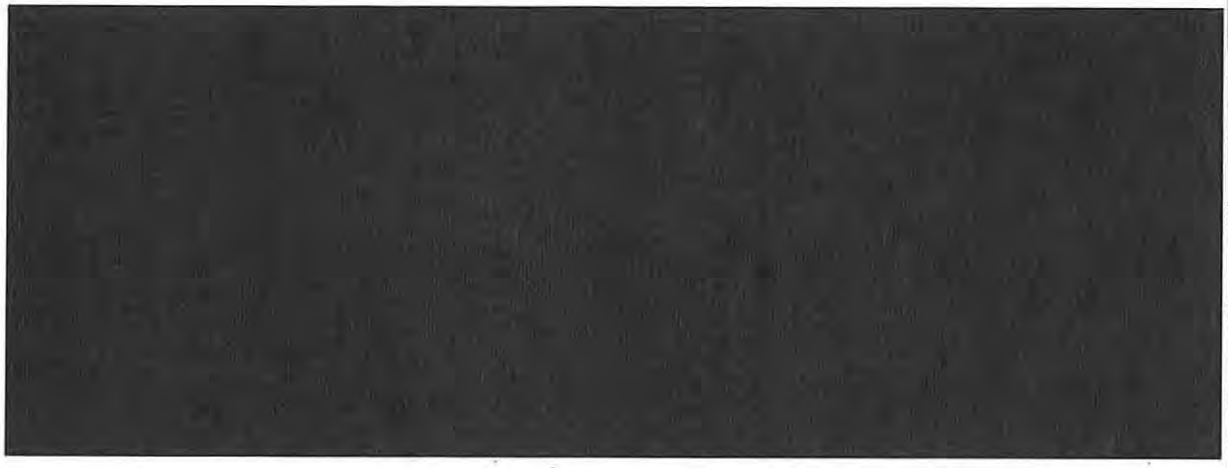
THE COURT: It will be done at least with respect to the first part of 3(b)(1) at the earliest practical point, but at least five years --

(b)(6); (b)(7)(C) [redacted]: No later than five years.

THE COURT: No later than five years. And I understand that five years has been a time frame that has appeared in other procedures, but I think it probably would be helpful to just sort of talk a bit about where that comes from, why is that a number that's been selected.

(b)(6); (b)(7)(C) [redacted]: NSA can correct me if I'm wrong; the five years comes from the fact that [redacted]

[redacted]



That, I think, is the general thinking behind the five-year retention period. That's the potential analytical life cycle of a particular piece of information.

[redacted] Your Honor, this is [redacted] for the NSA.

THE COURT: Sure. Yes, sir.

[redacted] In a couple of other places in our minimization procedures, namely in Section 5 and Section 6, we talk about the five-year rule where in certain cases the intelligence director may extend that in the case of domestic communications or in the case of U.S.-person information if again it has foreign intelligence value or evidence of a crime.

So in 3(b)(1) we talk about five years, but there are a couple of other sections that might be invoked by our SID director where he could extend it.

THE COURT: Yes. Well, I think this makes clear that it's not talking about things that are not relevant -- it's only talking about things that are not relevant to the authorized

purpose of the acquisition and not containing evidence of a crime. So the implication is that if it does do that, the five years may not necessarily be -- fair enough.

All right. Number 13, page 11 of your response from yesterday. Now, I had a couple of questions with respect to the three minimization procedures and what they say about the director being able to do certain things, but (b)(6); (b)(7)(C), I understand that you alerted the staff before the hearing that there's another potential issue that you have thought of that could impact this issue.

(b)(6); (b)(7)(C) Correct. There's a provision in the FISA that was recently changed, 1806(i), which basically says -- the previous iteration of that provision of the statute said if you are unintentionally acquiring radio communications when the sender and all intended recipients are located in the United States, the attorney general has to determine whether or not that piece of information can be retained in very extreme circumstances, otherwise such circumstances have to be destroyed upon recognition.

The recent FISA Amendments Act struck "radio" out of that provision such that the provision appears to on its face apply to all types of acquisitions conducted under the act. Whether or not that particular provision applies to this type of collection such that it would require us to basically destroy domestic communications as they are recognized is an issue that

we're still trying to work through.

THE COURT: Okay. All right. And I'm sure we'll continue to talk on that as you work it through, and thank you for alerting us to that. Let me go forward, though, with the minimization procedures as they are, and let me ask a couple of questions about them, putting aside for the moment this issue with 1806.

We had one question for you, and now I don't know if we asked you this before, but the one question was the NSA and the CIA procedures had the directors doing things in writing. And the FBI provision didn't say "in writing," but as I understand it, the FBI, as you cite here, has represented that any such determination by the director would be made in writing even if not expressly required.

(b)(6); (b)(7)(C): Correct.

THE COURT: Okay. That answers that. Another similar kind of question. There may be no significance to the difference in language, but the NSA procedures at page 5 say, and I'm paraphrasing because I don't have the exact quote, that unless the director "specifically determines" something.

And then the FBI provisions simply say "unless the director determines," and I think the CIA also says "unless the director determines." Is there any meaning I'm supposed to take from "specifically?"

(b)(6); (b)(7)(C): No. I think "specifically" was just

intended to capture the notion that this would be on a case-by-case basis as opposed to just a broad-base, I'm going to exempt this particular gigantic class of communications.

THE COURT: But I take it the FBI and a CIA would also be on a case-by-case basis.

[redacted] Yes.

THE COURT: Yeah, I didn't think it had a lot of significance, but you never know, so I thought I'd ask.

You know, I may be at the end of my list. What I'd like to do is take a break. But since there's fewer of us than of you, we will step out, and then you can stay here and if -- because there's a lot of people here.

Obviously, use the time. If something was said here that you have an issue with because, you know, at least from your experience it doesn't work that way, please talk among yourselves and we can straighten that out. Or, if I had asked a question and you say, *Gee, I think the best answer is X and nobody said X*, please feel free to tell [redacted] and we can get that better answered on the record.

Okay. Thanks, everybody. Just give us a few minutes.

(Recess taken.)

THE COURT: Just a couple things. Going back to the *abouts*, if we can go back to them for a moment, you know the Court will have to do, obviously, a Fourth Amendment analysis in terms of the reasonableness -- of all the procedures, not just

of the *abouts*.

But I guess my question is, is there a different analysis for the *abouts* than for the *to* or *from*? Or to put it another way, could somebody articulate for me what you believe why the *abouts* don't present a different Fourth Amendment issue from the *to's* and the *froms*, that it's the same issue?

Again, to amplify even a little more, is the possibility of acquiring information that otherwise it would not be permissible to acquire in the *about* scenario different from the *to* or *from*?

In other words, is it incidental? Would you describe it in that way? If not, how would you describe it? Is it any less or more likely to happen with the *abouts* than with the *to* or *from*? Or any other aspect of the Fourth Amendment analysis that you think is relevant.

(b)(6); (b)(7)(C) I don't think that the Fourth Amendment analysis is any different with respect to an *abouts* communication or *to* or *from*. I mean, it's just as likely that one end of a *to* or *from* could be a U.S. person in communication with a target as an *about*.

In either case, the U.S.-person information contained in that communication would be subject to the minimization procedures, and it's not that U.S. person that is the target of the acquisition of that particular communication; it is the user of the targeted selector that appears in the body of that communication. So I think for Fourth Amendment purposes, with

respect to U.S. persons, I don't think the analysis is any different.

MR. OLSEN: We have given some thought to this, because *abouts* collections has been an issue in this collection as well as prior court orders. But I just would reiterate what [redacted] said in terms of our view of it in that it's essentially for the Fourth Amendment purposes an incidental collection where the target is the targeted account, and to the extent that a U.S. person's communication -- to or from a U.S. person, that would be deemed to be incidental to the collection.

And therefore under the analysis we put forward in, for example, the Yahoo litigation, that would be permissible and reasonable under the Fourth Amendment as long as minimization procedures are appropriately applied.

THE COURT: Is it more or less likely to pick up U.S.-person information in an *about* than a *to* or a *from*?

MR. OLSEN: I don't know the answer in practice. At least from my perspective in theory, I wouldn't see why it would be more likely than a targeted *to* or *from* collection where the target's outside the United States where there's similarly the possibility that that target would be in communication with someone in the United States, with a U.S. person in the United States.

So, just analytically, I think the same incidental collection subject to minimization procedures framework would

apply. And so under the Fourth Amendment applying, that we would submit would be reasonable under the Fourth Amendment.

(b)(6); (b)(7)(C) And I would note that in his opinion on the Yahoo litigation, Judge Walton recognized the reasonableness of a presumption that non-U.S. persons located overseas are more likely to communicate with other non-U.S. persons located overseas which may bear on the volume of potentially -- or *abouts* communications that potentially implicate U.S. persons versus non-U.S. persons. I think if you apply that presumption, it's more likely that an *about* will not implicate U.S.-person information.

THE COURT: Okay. Fair enough.

Well, that's really all that I --

(b)(6) Judge, I'm sorry.

THE COURT: Yes. Go ahead, (b)(6)

(b)(6) With regard to the *abouts*, it's occurred to me, just to be clear on the record, there were [redacted] sort of subcategories of such communications that were laid out in a footnote to Judge Kotelly's opinion in the PAA that in turn I think referred to an opinion issued or an order issued by Judge Vinson last year.

Do those [redacted] categories, as previously set out in those places, continue to be accurate and up to date and complete in terms of the communications that are obtained?

[redacted] I think so. If I recall correctly, and I

may not have all [redacted] categories off the top of my head, we have the instance where the selector is mentioned in the body of an e-mail sent between two communicants.

You have an instance where [redacted]

THE COURT: Well, there was [redacted]

[redacted] (b)(6); (b)(7)(C): Oh, [redacted] yes.

(b)(6) [redacted] And [redacted]

(b)(6); (b)(7)(C) [redacted]

(b)(6) [redacted]

[redacted] Yes.

THE COURT: Okay. Thank you, (b)(6), for that. Appreciate it. So I guess the only other outstanding issue at the moment is the 1806, I'll call it, issue, and what is your thinking in terms of timing? Obviously, at this point at least we have the September 4 deadline that we're looking at, but what are your thoughts on timing?

MR. OLSEN: We're going to turn to this immediately

following the hearing. This has been, as I think (b)(6); (b)(7)(C) mentioned, been an issue we identified yesterday or the day before in the evening.

So we have the right folks here to talk about it, and my expectation first would be that we would be able to communicate directly with the Court staff. I don't know how quickly we will have a definitive answer, but I would expect that we will have a definitive answer, understanding the timing of this overall, by tomorrow at some point and that what I expect to do is to have something in writing, perhaps not very formal, something along the lines of what we recently gave to the Court to address this issue.

It may be that that will be, in terms of our view, that we think we have a resolution to the issue and that no further action is necessary. It may be that we have other steps to propose to the Court, but we certainly understand the importance of moving quickly and turn to this right away.

THE COURT: Okay. Fair enough.

(b)(6); (b)(7)(C) And there were three other issues that we'd just like to clarify, statements that were made previously that we just want to provide maybe a fuller context to.

THE COURT: Sure.

(b)(6); (b)(7)(C) With respect to oversight and the number of compliance incidents that we've identified, just to give you some perspective on the relative nature of that number, since

the acquisition of the Protect America Act began, NSA has tasked over [redacted] selectors. So the fact that we've identified [redacted] or so actual compliance incidents is, relatively speaking, a very, very small number.

Another point that we'd just like to provide a little more clarification on is the point that [redacted] made with respect to extending the five-year retention period for particular communications, and maybe [redacted] can expand on this a little bit more.

We just want to make it clear that with respect to the determination by the SID director to extend that, that's not on a communication-by-communication or selector-by-selector basis. It can be a broader range of communications that the SID director may make that determination for and extend the retention period.

THE COURT: Are you focusing on a particular part of the procedures? Can we look at them? That will help me, I think. These are the NSA minimization procedures?

(b)(6) [redacted] It's section 6(b).

(b)(6); (b)(7)(C) [redacted] There's one in 6(b), and there's one in 5(3)(b).

(b)(6) [redacted]: May I ask a question?

THE COURT: Absolutely. Go ahead, (b)(6) [redacted]

(b)(6) [redacted] Has the SID director invoked this provision? Is there an extension currently in place?

[redacted]: There's not under PAA. [redacted]

[redacted]

[redacted]

(b)(6) [redacted]

[redacted]

[redacted]: [redacted].

(b)(6) [redacted]: Oh, I see.

[redacted]: [redacted]

[redacted] Our concern, we don't want to leave a misimpression, when you read this together, if we discover -- if we find that there are U.S.-person communications here, we will take this action.

If, however, we haven't discovered that and the SID director extends the period, it's possible it will be undiscovered U.S.-person communication during that seven-year period. So we don't want to give a misimpression by saying retained no longer than five years in any event.

I guess it should be read to say in any event -- I don't know where it is, but it allows the SID director to extend the retention period as invoked. In that case, undiscovered. We haven't realized it, but we have these kinds of communications. They would continue to be retained as well.

THE COURT: That's because they're undiscovered. If it's discovered, it's five years.

MR. [redacted]: That's correct. If it's discovered --

THE COURT: Yeah. If they're discovered.

[redacted] They would be destroyed at that time.

THE COURT: Obviously, if they're not -- okay.

(b)(6); (b)(7)(C), now that I've read them again, can you just repeat what you said you wanted to make clear, that this wasn't on a case-by-case basis?

(b)(6); (b)(7)(C) It can apply to a broader range of communications. It's not, okay, the SID director determines that this --

THE COURT: Particular little thing right there.

(b)(6); (b)(7)(C) -- meets this standard, therefore I can extend the retention duration beyond the five years. It can be a range of communications.

THE COURT: Just give me an example. I think we just had one. Can somebody give me an example?

[redacted]

THE COURT: I see. Okay. Thank you.

(b)(6); (b)(7)(C) And one last clarification. With respect to the ongoing requirement that an analyst keep track of its targets and basically is responsible for ensuring the continuing foreign intelligence purpose of the collection, [redacted] said NSA imposes a [redacted] that the analyst has to make that determination.

We just want it to be clear that that is the outer limit of the requirement that that determination be made and that in practice that determination is made on a much more ongoing basis than just [redacted]

THE COURT: And I don't think I understood it to mean [redacted] but I appreciate that clarification.

All right. Anything else?

(b)(6); (b)(7)(C) That's all, Your Honor.

THE COURT: Okay. Thank you so much, everybody. I appreciate it. All right. We are adjourned.

(Proceedings adjourned at 11:02 a.m.)

(b)(6) Deputy Clerk
FISC, certify that this document is a true and correct copy of the original. (b)(6)

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix V

2012 IEEE 26th International Parallel and Distributed Processing Symposium Workshops & PhD Forum

A Stream Reassembly mechanism based on DPI

Shuhui Chen
College of Computer Science
National University of Defense Technology
Changsha, China
Email: shchen@nudt.edu.cn

Yong Tang
College of Computer Science
National University of Defense Technology
Changsha, China
Email: ytang@nudt.edu.cn

***Abstract*—Stream Reassembly is an indispensable function of Deep Packet Inspection, which is an critical element of Network Intrusion System. However, since it need to heavily move packet payload from one block of memory to another block of memory, Stream Reassembly has a serious memory performance issue. In this paper, in order to improve the Stream Reassembly performance, a Stream Reassembly Card (SRC) is designed, which enables to manage and assemble streams through adding a level of buffer to adjust the sequence of packets by using the Multi-core NPU. Specifically, three optimistic techniques, namely Stream Table Dispatching, No-Locking Timeout, and Multi-channel Virtual Queue are introduced in SRC design. The experiments show that the reassembly can achieve more than 3 Gbps in terms of processing speed, triply outperforming over the traditional server based architecture.**

***Index Terms*—Network Security; Network Intrusion System; Network Forensics System; Multi-core NPU; Stream Reassembly;**

I. Introduction

DPI (Deep Packet Inspection) is a critical technique for Network Forensic System (NFS), where packet payloads need to be matched against pre-defined patterns to obtain the evidences with a 4-step process, namely preprocessing, header-matching, content-matching and outputting in NIDS and NFS. In general, in the event of a network with a low speed, server based approach (in which the stream reassembly, rule matching and warning are all conducted by one server) can satisfy the performance requirement. However, with the exponential increasing of bandwidth, the traditional server based approach (even for a server with high performance) no longer meets the performance requirement. To break up this bottleneck, many researches have been carried on to improve the overall performance by achieving efficient content-matching [1]–[6].

Many previously reported methods mainly focus on improving the rule matching algorithms, and/or using FPGA [1], [2] or GPU [3]–[6] for efficient content-matching, and the results show that the ratio of running time used for matching is decreasing with the enhancement of matching performance. Experiments from some other researchers [7] further indicated that when the ratio of the matching time to the overall decrease to 1%, Stream4 (which reassembles streams in previous Snort version) will take on the load of 80% when it is used to assemble the packets.

Currently, advanced progresses have been made in the network electron component area. For example, Raza Micro-electronics has developed XLR, XLS and XLP NPUs, while Cavium has launched OCTEON Series NPU. The emergence of these multi-core NPUs can largely improve the performance of the network devices and network security devices. In this paper, we present a new Stream Reassembly Card (SRC) design, which enables to manage and assemble streams through adding a level of buffer to adjust the sequence of packets by using the Multi-core NPU.

II. Related Work

There are two open source programs: Libnids [8] and Tcpflow [9] that fulfill TCP stream reassembly, but both of them cannot meet the performance requirements of the current network links. Researchs having relationship with stream are often focus on the measurements.

For example, [10] has used two data recorded from two different operational networks, and studied the flows in size, duration, rate and burst, and examined how they are correlated. [11] concerned on the problem of counting the distinct flows on a high speed network link. They proposed a new timestamp-vector algorithm that retains the fast estimation and small memory requirement of the bitmap-based algorithms while reducing the possibility of underestimating the number of active flows.

[12] has introduced a TCP reassembly model and a stream verification methodology that can be used to derive and compute reassembly errors. [13] has introduced an algorithm that solves the problem of TCP stream reassembling and matching performance problem for network forensics system and IDS. Instead of caching the total fragments, their methods stores each fragment with a two-tuple that is constant size data structure, thus the memory requirement involved in caching fragments is largely reduced.

[14] has introduced a hardware based reassembly system to solve both the efficiency and robust performance problems in the face of the adversaries to subvert it. They characterized the behavior of out-of-sequence packets seen in benign TCP traffic, and designed a system that addresses the most commonly observed packet-reordering case in which connections have at most a single sequence hole in only one direction of the stream.

III. Why Multi-core NPU is Selected

NIDS obtains copies of packets directly from the network media, regardless of their destination. Raw packets captured

978-0-7695-4676-6/12 $26.00 © 2012 IEEE
DOI 10.1109/IPDPSW.2012.152

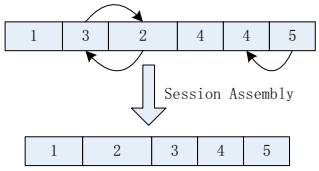


Fig. 1. An example of stream reassembly.

by the NIDS are confused and disordered messes, but DPI in NIDS needs these packets to be fabricated as integrated blocks according to their TCP stream belongings before they are sent to the matching engine.

Figure. 1 gives an instance, and the stream in the example is composed of 6 packets. But packet 2 and packet 3 are out of order, and packet 4 is repeated. The stream reassembly process needs to exchange the sequence of packet 2 and packet 3, and the unwanted second packet 4 should also be deleted. The process incurs 3 times packets movement: packet 2 moving ahead, packet 3 moving backwards, and packet 5 moving ahead. This is just an example of a single stream, and in the real network environment, one backbone link may contain a large number of streams. In other words, there may be too many packet movements in the reassembling process. Modern servers use DRAM (DDR2 or DDR3) as their main memory, one memory access may take a number of cycles to obtain a result because DRAM has a relatively long startup time.

However, multi-core NPU can improve the performance of this kind of operation, which is because:

(1) There are many hardware threads in one core and many cores in one NPU, which makes the total threads in a NPU, will be more than a dozen. The threads of this kind are hardware threads instead of software threads so the switching cost is very low. The large number of hardware contexts enables software to more effectively leverage the inherent parallelism exhibited by packet assembling applications. When one thread is waiting for the result of the memory accessing, the other thread could switch in and makes another memory accessing request, and if many threads use such a pipeline, the latency of the DRAM will be hidden and the effective bandwidths of the DRAM access would increase.

(2) A multi-core NPU is often with low electric power consumption, so it is easy to be manufactured as a card. When a NPU based card is used, an extra buffer is introduced to the processing flow, so the packets can be sorted as they are being transferred from the memory of the card to the memory of the host (server), which is a form of trading space for performance. In this way, when the packets have been received into the memory of the card, they are stored in the memory as their reaching order, but their sequence are maintained by the software running on the NPU.

(3) The architecture of NPU often has a favorable I/O features, and the packets could be imported from the interface to the memory with high throughput. As the dispatching component generally dispatch packet according to the selected bits from the packet head, stream reserved would not be a problem. Since many researches [15], [16] focus on how to accelerate the packets capturing performance, an approach combination packets capture and stream reassembly is cost-effective.

(4) NPU often has a well designed message-passing mechanism between different threads, which uses cross-bar structure or fast shared SRAM as its transferring medium, and makes the cooperation and synchronization between threads facile.

IV. System Architecture

A. Stream in TCP Transferring Level

We focus on three different critical actions, which are TCB creation (the point at which an IDS decides to instantiate a new TCB for a detected connection), Packet Reorder(the process an NIDS uses to reconstruct a stream associated with an open TCB), and TCB Termination (the point at which the IDS decides to close a TCB). Every TCP connection can be expressed as a four-element tuple (which includes source IP, source port, destination IP, and destination port). Once a packet is captured, its corresponding stream needs to be found and the TCB data structure needs to be updated. Basically, TCB is attached to a Hash Table indexed by hash algorithm using some bits from the four-element tuple as parameters. Collisions lead to several TCBs attached to one table entry.

B. Frameworks of SRC

The framework of SRC is depicted in Figure. 2. In SRC, packets are captured from the interfaces to the memory; for maintaining the TCP connection data, a hash table known as Stream Table is used. When the packets enter the memory, their locations are stored in the packet descriptions. Besides the points which point to the packets, packet descriptions also contain the packet length and the fields used to dispatch the packets to the threads.

Threads running on the NPU wait circularly, processing a received packet and then waiting for another packet. Once the data needs to be submitted, every thread is responsible for the task of submitting the packets from the memory of the NPU to the memory of the host. Both the softwares running on the NPU and CPU share a little memory space in the DDR of the NPU for message communication, and the memory space is used by the NPU to get the address of the DMA, the timeout of the host setting, the BlockSize, and the consuming states; CPU can also use the memory space to gain the running states of the NPU. As the packets are DMAed to the host memory, the transferring is conducted one packet after another, which is due to the packets are not stored consecutively in the memory of the NPU while we need them to be consecutive when they reach the memory of the CPU.

Software running on the NPU mainly executes three actions mentioned in Section. IV-A: TCB Creation, Packet Reordering, and TCB Termination. When a packet reaches one core, the related thread looks up the Stream Tables to determine whether there is a corresponding TCB exists. If not, the corresponding TCB is created, and the packet is appended to the TCB. Or else, the packet is appended to the corresponding TCB and its link position is determined; meanwhile, a judgment is made

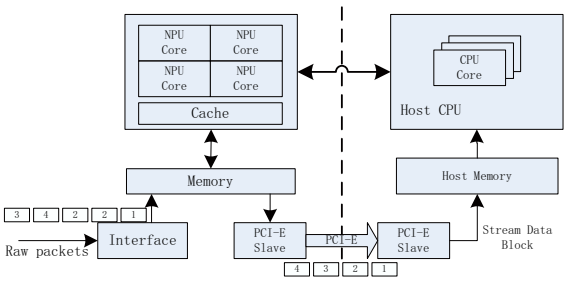


Fig. 2. Frameworks of SRC.

on whether the total packet size of the stream is equal or larger than BlockSize (Submitting Block Size). If the answer is positive, all the packets are submitted in the light of their sequence to the Host.

The total connection records are maintained in a hash table called Stream Table for efficient access. Note that the hash needs to be independent of the permutation of source and destination pairs, which could be achieved by comparison the source IP together with source port and destination IP together with the destination port, and always make the less one to be the first parameter or using some hash algorithms that are not sensitive to the sequence of parameters. Using such hash values as the indexes to the stream table, the corresponding connection can be located. Hash collisions can be resolved by chaining the colliding TCBs in a linked list.

Data submission procedure running by the packet processing threads needs to work cooperatively with the program running on the host CPU. A consecutive memory chunk needs to be allocated to storage the packets uploaded, and for the convenience of the packet organization, the chunk needs to be divided into fix-sized buffers which are organized as a ring. Software (IDS and NFS) running on host continually process the data block received.

C. The Procedures of Stream Reassembly

The two significant data structures in stream reassembly are stream table and TCB. Stream table is made up of many entries, each of which points to a list of TCBs that have the same hash value. In SRC, two types of threads are used to fulfill the stream reassembly: the packet processing thread and the timeout thread. The packet processing threads are responsible for packet receiving, stream reconstruction and data submission; moreover, stream reconstruction is divided into TCB Creation, Packet Reordering and TCB Termination. The timeout thread is a simple circular procedure; it accesses TCBs one by one ceaselessly, comparing the current time with the time of the last coming packet in every stream. If the gap between the two times is large than the appointed value, timeout thread deems that the corresponding stream may be asleep or dead, so it submits the remaining data and delete the TCB to give space to other streams.

The main purpose of *ReorderPacket* is to sort the one-stream-affiliated packets according to their TCP sequence number, and drop the repeated packets that have the same sequence number. Instead of being processed after a batch of packets belonging to a stream have been received, the packets are maintained their order upon being received. The reasons why it does in this way are as follows: (1) The batch processing could cause the computing burst, which is detrimental to the smooth process; (2) Disordered packets are rare actually, most of the arrived packets are ordinal and consecutive. As a result, processing packets one by one will save more computational resource.

As the data is submitted to the host, all the packets must be insured to be ordinal and consecutive. We use **ordering** to express the sequence of the packet and **continuity** to denote if there is any packet should reach but have not reached. When the packets reache, their ordering can be insured by sorting the sequence number and modifying the points of the list that attached packets, but the continuity cannot be ensured, it is due to the disordered arrival is available. To determine if the data can be submitted, a counter DisContinuity Number (DCN) is used to identify if the received packets is continuous or not. DCN is the counter of gaps between adjoining packets for a stream.

The larger the DCN is, the more the degree of discontinuity is. An example is given as follows: for one direction of a stream, if packets 1, 2, 3, 4, 5, and 7 have been received (the numbers are the order numbers of the packet been sent out, not the sequence numbers of the TCP level), the DCN of the stream is 1, because there is a gap between packet 5 and packet 7. If packets 1, 2, 3, 4, and 7 have been received, the DCN of the stream is still 1, because even through there are two packets between packet 4 and packet 7 as they look like, we do not know there is one packet or two packets can fill in this gap when we receive the packet 7, the only fact we know is that there is a gap between the sequence number of packet 4 and packet 7 from TCP level.

All the packets are linked up while the packets with smaller sequence number are in the front of the link and the packets with bigger sequence number are at the back of the link. Bidirectional links for the packets are needed, because packets needed to submitted from NPU to CPU according to the sequence number of the packets. But when a packet arrivals, locating the inserting point from the verse direction may gain better performance. That is because the gap exists scarcely; and even when it emerges, it will be filled up quickly.

When a stream ends, timeouts or its size exceeds the BlockSize, the packets belong the stream must be uploaded to the CPU. Under the circumstances of stream end or timeout, DCN will be zero if all is OK. If it is not zero for some packets have not been received, there is nothing can be done by the reassembly component. But if we are under the third circumstance, which shows that the size of the stream achieves the BlockSize, and the DCN is not zero, reassembly component needs to find the gap that causing the DCN to be not zero. We can look for the link of the stream, if the lost packets are far from the last packet (for example, 8 packets is an experiential value), the finding process is stopped and the packets are submitted, considering that packets will not arrive.

On the other hand, if the gap is among the last 8 packets, we will submit the integrated packets and maintain the remanent inconsecutive packets of the stream. To sum up, we try to upload the packets that are consecutive to the host.

V. Improvement

A. Stream Table Dispatching Technique

There are two techniques can be implemented to organize the TCB in the stream table: shared stream table and separated stream table. For the shared stream table, all the threads share a whole stream table, so all the threads need to access the stream table in the global memory. As a result, a lock must be added to the corresponding item of the stream table when one thread is processing the packet. The contest accessing by all means decrease the performance. And for the separated stream table, every thread uses its own stream table, and we must use more memory than the shared stream table to hold several tables to make the TCB list not too long.

So, if both high utilization and high performance are required, a new technique must be adopted. To solve this problem perfectly, a unified hash method for packet dispatching to the threads and obtaining the stream table index is applied, making all the TCBs have the same stream table index are dispatched to the same thread. Therefore, the items of the stream table need not to append locks because all the packets hashed to the special item will be processed by one special thread. In addition, if the stream table items assigned to every thread are consecutive and their size is aligned to the Cache blocks, then the Cache hit ratio will be high to improve the overall performance.

B. No-Locking Timeout

A large numbers of concurrent TCP streams are present in the network, so the states of a large number of TCBs attached to the stream table must be maintained. To release the memory space of the streams that are not active in the SRC, three submission schemas have been used: stream timeout, stream termination, and the size of packet buffered achieve a specified size.

Because the packets timed out have to be uploaded, a separated timeout thread is used to confirm whether there is any stream is time out. The timeout thread circularly obtains every item in the stream table and then gains every TCB in the link to determinate if there is a timeout. If a timeout occurs, submission the packets and deletion the TCB are conducted. The stream table and the TCBs become the critical resources and locks are required because that the packet processing threads need to process on the TCBs and their corresponding packets as same as the timeout thread does.

The lock operation should be removed as our experiences on the network device and network security devices because we have not so much time to process a packet. For example, we only have 300 ms to process a packet for a Gbps link [17]. For the multi-cored NPUs of RMI and OCTEON, they both have a fast messaging mechanism to implement the synchronization and information transformation among different threads. The messaging mechanism can be used to remove the locks by the timeout thread sending a message to the packet processing thread, and then the packet processing thread submitting the packets and deleting the TCBs.

C. Multi-channel Virtual Queue

The performance of the Packet capture is critical to the overall traffic analysis system [18], [19]; similarly, data block submission is critical to the overall system of stream reassembly. It is obvious that multi-core computers are the current dominant trend in computers; thus, how to avoid data coping and make the data block distributed to the several cores in the host evenly can bring distinct improvement to the overall performance.

Luca [16] exploits the feature of the Intel NIC, but he has overtaken that packets on different directions for one stream will be dispatched to different core (Matching Engineer), many attacking warnings will not be reported for this reason. We have ever amended this problem by allowing the driver to re-compute the hash value if the source address is bigger than destination address, and if the source address is less than destination address, hardware distributing mechanism is kept. But it impacts the performance, although it is stream based, the performance of the method is only 60% of the method [16] introduced. Furthermore, Intel NIC only has 4 fixed queues, but the latest CPU can support 8 cores, the packets in 4 queues cannot be dispatched to 8 cores.

The host creates several ringed buffers, and tells the program running on the embedded multi-core NPU the number of ringed buffers, ring descriptors, length, head and tail pointers of the ring through shared memory. NPU then calculate the corresponded queue that each stream data block will be dispatched according to the information given by the CPU.

VI. Implementation and Performance Evaluation

A. Implementation

A Stream Reassembly Card is developed using XLS416 produced by Raza Microelectronics, Inc (RMI). The RMI XLS416 is a multi-core, multi-thread MIPS64 processor with a rich set of integrated I/O. XLS 416 has 4 cores and every core has 4 threads, so the total thread number is 16. One thread (referred as timeout thread) is used to take charge of the timeout management, and the other threads (referred as packet processing threads) all execute the same routine, whose job is receiving packets, assembly, and submission, when the timeout thread find that any stream has been timed out, it will send a message to the corresponding thread to notify which stream has been timed out, then every packet processing thread circularly check if there is any timeout message after processing one packet.

XLS 416 has three frequency models: 800M, 1.0G and 1.2G; for the best of the performance, we used the XLS with 1.2G Hz. XLS 416 integrates eight Gigabit Ethernet or two Ten Gigabit Ethernet. To further save the PCB size and consider that the Ten Gigabit Ethernet may be the mainstream link of the campus network, 2 ten-Gigabit interfaces are adopted to

SRC. Our SRC has 4G DRAM with 533 MHz and 1 PCIe1.1 × 4 Bus used to connect to the host. The interface chip is VSC8486-11 that connect the fiber module and the XLS through XAUI. DIMM chips are used instead of DIMM strips, for it occupies less PCB space and the stability is better. The total chip's power consumption is under 26 watts.

In the software level, there are a stream reassembly program running on the SRC and a Driver running on the host. Program running on the SRC is bound to one Image with the RMI OS and is burned into the Flash, which is also used to boot the system. We provide an SRC_API extending from Libnids. In addition to the feature of the Libnids, our SRC_API can be used to obtain the statistics and set the number of the analyses threads running on the host, timeout of the stream, and the BlockSize. 2M space is used to share information by the CPU and NPU, and 64M byte space per capturing thread running on the CPU.

B. Evaluation

The test topology is depicted in Figure. 3. Dell PowerEdge R710 Server with an Xeon 2.13Ghz E5606 CPU, and total 16GB ECC DDR3 (4x4GB) is used to host the SRC. R710 Server has a PCIe × 8 Bus which can be used to hold the joint of the SRC. Red Hat Enterprise Server 64Bit with a 2.6.18-92.el5 kernel is used as the Operation System. An IXIA XM2 with an Xcellon-Ultra NP 10GbE Load Module is used to construct the evaluation environment. The application level test is carried out by IXIA XM2 [20].

The HTTP is used as the traffic load. Two XM2 ports are used to emulate the traffic between one server and multi-clients. To make use of the transferring bandwidth fully, 8 capture threads in the host are used. To gain the relationship between the NPU core number and stream reassembly performance, we test the performance under different core number circumstance. Since every core has 4 threads, when one core is tested, one thread is used as timeout thread and the other 3 threads are used to reorder the packets; and when two cores are tested, one thread is used as timeout thread and the other 7 threads are used to reorder the packets, and so forth. Because the traditional NIDS used Libnids [8] to conduct its stream reassembly, we tested its performance and the results are depicted in the last column of Table. I.

More cores lead to higher performance, and longer packets produce higher performance. It is also revealed that if all the cores are used, the performance is close to that of the packet capture. It means that when all the threads in the NPU are turned on to reassemble the packets, the performance is near to the PCI transferring ability, so it can be inferred that if the PCI multiplying factor is 8, the performance will be higher than the current implementation. As we know, the average packet length is between 300 and 400 bytes, so the performance of the real environment will be higher than 3Gbps. That is to say, while we formerly used three high performance server to conduct the stream reassembly, now one SRC can accomplish the same task.

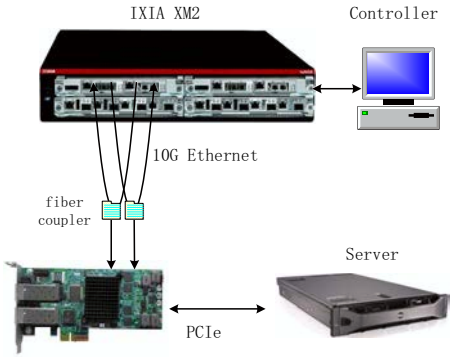


Fig. 3. Stream Reassembly Performance Test Environment.

TABLE I
THROUGHPUT OF SRC AND LIBNIDS.

Packet Length[1]	1 core	2 cores	3 cores	4 cores	Libnids
64	0.22	0.33	0.61	0.64	0.45
128	0.25	0.47	0.98	1.18	0.48
256	0.59	1.02	2.50	3.11	0.82
512	0.75	1.51	2.66	3.48	0.93
1024	1.30	2.73	3.12	3.70	0.99
1500	1.45	2.98	3.11	3.85	1.21

[1] Unit: Byte.

VII. CONCLUSION

The performance of TCP packet reassembly becomes the bottleneck as the matching performance is increasing. In this paper, a co-processing stream reassembly framework based on multi-core NPU has then been introduced as a card, so the packet capture and stream reassembly can be both solved by a card. And to heighten the performance, we brought forward Stream Table Dispatching, No-Locking Timeout, and Multi-channel Virtual Queue to improve the performance of the proposed SRC scheme. The solution adopted cannot hold much memory because the size and electricity limit, whereas the memory size is critical to the performance, we analyzed how much memory is need for a specified timeout, block size and throughput. Last, RMI XLS416 was used to implement a co-processing Stream Reassembly Card, The result showed that our scheme is about 3 times of Libnids used in the current predominant server.

VIII. ACKNOWLEDGMENT

This work has been supported by the National High-Tech Research and Development Plan of China under Grant No.2011AA01A103 .

REFERENCES

[1] N. Weaver, V. Paxson, and J. M. Gonzalez, "The shunt: an fpga-based accelerator for network intrusion prevention," in *Proceedings of the 2007 ACM/SIGDA 15th international symposium on Field programmable gate arrays*, ser. FPGA '07. New York, USA: ACM, 2007, pp. 199–206.

[2] M. Labrecque and J. G. Steffan, "The case for hardware transactional memory in software packet processing," in *Proceedings of the 6th ACM/IEEE Symposium on Architectures for Networking and Communications Systems*, ser. ANCS '10, 2010, pp. 37–48.

[3] V. Giorgos, A. Spiros, P. Michalis, E. P. Markatos, and S. Ioannidis, "Gnort: High performance network intrusion detection using graphics processors." in *Proceedings of the 11th international symposium on Recent Advances in Intrusion Detection.* USA: SpringerLink, 2008, pp. 116–134.

[4] G. Vasiliadis, M. Polychronakis, S. Antonatos, E. P. Markatos, and S. Ioannidis, "Regular expression matching on graphics hardware for intrusion detection," in *Proceedings of the 12th International Symposium on Recent Advances in Intrusion Detection*, ser. RAID '09, Berlin, Heidelberg, 2009, pp. 265–283.

[5] G. Vasiliadis, M. Polychronakis, and S. Ioannidis, "Midea: a multi-parallel intrusion detection architecture," in *Proceedings of the 18th ACM conference on Computer and communications security*, ser. CCS '11. New York, USA: ACM, 2011, pp. 297–308.

[6] C.-H. Lin, C.-H. Liu, and S.-C. Chang., "Accelerating regular expression matching using hierarchical parallel machines on gpu," in *IEEE Globecom 2011 proceedings*, HOUSTON, TEXAS, USA, pp. 1–5.

[7] S. Egorov and G. Savchuk, "Snortran: An optimizing compiler for snort rules," *Fidelis Security Systems*, 2002.

[8] Libnids, http://libnids.sourceforge.net/.

[9] Tcpflow, http://afflib.org/software/tcpflow.

[10] K. chan Lan and J. Heidemann., "A measurement study of correlation of Internet flow characteristics," *Computer Networks*, vol. 50, no. 1, pp. 46–62, 2006.

[11] H.-A. Kim and D. O'Hallaron, "Counting network flows in real time," in *Global Telecommunications Conference, 2003. GLOBECOM '03. IEEE*, vol. 7. IEEE, dec. 2003, pp. 3888–3893.

[12] G. Wagener, A. Dulaunoy, and T. Engel, "Towards an estimation of the accuracy of tcp reassembly in network forensics," in *Future Generation Communication and Networking, 2008. FGCN '08. Second International Conference on*, vol. 2. IEEE, dec. 2008, pp. 273–278.

[13] M. Zhang and J. Ju, "Space-economical reassembly for intrusion detection system." *Information and Communications Security*, pp. 393–404, 2003.

[14] S. Dharmapurikar and V. Paxson, "Robust tcp stream reassembly in the presence of adversaries," in *Proceedings of the 14th conference on USENIX Security Symposium - Volume 14*, Berkeley, CA, USA, 2005.

[15] E. M. L. Gorka Aguirre Cascallana, "Collecting packet traces at high speed," 2006.

[16] L. Deri, N. S. P. A, V. D. B. Km, and L. L. Figuretta, "Improving passive packet capture: Beyond device polling," in *Proceedings of SANE*, vol. 2004, pp. 85–93.

[17] J. V. Lunteren, T. Engbersen, and S. Member, "Fast and scalable packet classification," *IEEE Journal on Selected Areas in Communications*, vol. 21, pp. 560–571, 2003.

[18] L. Deri, "ncap: Wire-speed packet capture and transmission," in *End-to-End Monitoring Techniques and Services, 2005. Workshop on*. IEEE, 2005, pp. 47–55.

[19] M. Smith and D. Loguinov, "Enabling high-performance internet-wide measurements on windows," in *PAM*, 2010, pp. 121–130.

[20] IXIA, http://www.ixiacom.com/.

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix W

US008813221B1

(12) **United States Patent**
Dubrovsky et al.

(10) **Patent No.: US 8,813,221 B1**
(45) **Date of Patent: *Aug. 19, 2014**

(54) **REASSEMBLY-FREE DEEP PACKET INSPECTION ON MULTI-CORE HARDWARE**

(75) Inventors: **Aleksandr Dubrovsky**, San Mateo, CA (US); **John E. Gmuender**, Sunnyvale, CA (US); **Huy Minh Nguyen**, Fountain Valley, CA (US); **Ilya Minkin**, Los Altos, CA (US); **Justin M. Brady**, San Jose, CA (US); **Boris Yanovsky**, Saratoga, CA (US)

(73) Assignee: **SonicWALL, Inc.**, San Jose, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1015 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **12/238,205**

(22) Filed: **Sep. 25, 2008**

(51) **Int. Cl.**
G06F 11/00 (2006.01)

(52) **U.S. Cl.**
USPC **726/22**; 726/23

(58) **Field of Classification Search**
CPC H04L 47/34; H04L 63/14; H04L 63/1416; H04L 63/145; H04L 45/00; H04I 63/1408; G06F 21/00
USPC 726/22, 23
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,796,942	A	8/1998	Esbensen	
5,945,933	A	8/1999	Kalkstein	
6,088,803	A	7/2000	Tso et al.	
6,108,782	A	8/2000	Fletcher et al.	
6,119,236	A	9/2000	Shipley	
6,178,448	B1	1/2001	Gray et al.	
6,219,706	B1	4/2001	Fan et al.	
6,449,723	B1	9/2002	Elgressy et al.	
6,851,061	B1	2/2005	Holland et al.	
7,134,143	B2	11/2006	Stellenberg et al.	
7,185,368	B2	2/2007	Copeland, III	
7,304,996	B1	12/2007	Swenson et al.	
2002/0083331	A1	6/2002	Krumel	
2003/0084328	A1	5/2003	Tarquini et al.	
2003/0110208	A1 *	6/2003	Wyschogrod et al.	709/202
2003/0145228	A1	7/2003	Suuronen et al.	

(Continued)

FOREIGN PATENT DOCUMENTS

EP	1 122 932	8/2001
EP	1 528 743	5/2005
WO	WO 97/39399	10/1997

OTHER PUBLICATIONS

Villa (Feb. 2008). IBM Research Report: Too many words, too little time: Accelerating real-time keyword scanning with multi-core processors. Retrieved from http://domino.research.ibm.com/library/cyberdig.nsf/papers/9EB4740B4B0739CF852573F5005A6311/$File/rc24488.pdf. Retrieval data Mar. 5, 2012.*

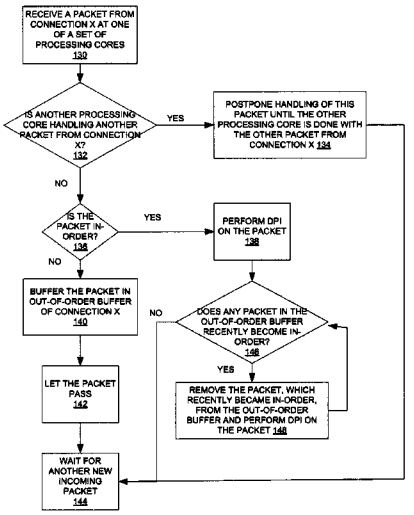
(Continued)

Primary Examiner — Brian Shaw
(74) *Attorney, Agent, or Firm* — Lewis Roca Rothgerber LLP

(57) **ABSTRACT**

Some embodiments of reassembly-free deep packet inspection (DPI) on multi-core hardware have been presented. In one embodiment, a set of packets of one or more files is received at a networked device from one or more connections. Each packet is scanned using one of a set of processing cores in the networked device without buffering the one or more files in the networked device. Furthermore, the set of processing cores may scan the packets substantially concurrently.

16 Claims, 7 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

2004/0093513	A1	5/2004	Cantrell et al.	
2004/0123155	A1	6/2004	Etoh et al.	
2004/0255163	A1	12/2004	Swimmer et al.	
2005/0120243	A1	6/2005	Palmer et al.	
2005/0216770	A1	9/2005	Rowett et al.	
2005/0262556	A1	11/2005	Waisman et al.	
2006/0020595	A1	1/2006	Norton et al.	
2006/0069787	A1	3/2006	Sinclair	
2006/0077979	A1 *	4/2006	Dubrovsky et al.	370/394
2007/0058551	A1	3/2007	Brusotti et al.	

OTHER PUBLICATIONS

"The Ultimate Internet Sharing Solution, WinProxy, User Manual," Copyright 1996-2002 Osistis Software, Inc., dated Feb. 2002 (290 pgs).

Roesch, Martin and Green, Chris, "Snort Users Manual," Snort Release 2.0.0, M. Roesch, C. Green, Copyright 1998-2003 M. Roesch, Copyright 2001-2003 C. Green, Copyright 2003 Sourcefire, Inc. dated Dec. 8, 2003 (53 pgs).

Bellovin, S., "Firewall-Friendly FTP," Network Working Group, RFC No. 1579, AT&T Bell Laboratories, Feb. 1994 , http://www.ietf.org/rfc1579.txt?number=1579, downloaded Jul. 15, 2002, 4 pages.

European Search Report, Application No. EP 04 02 5579, May 23, 2005, 3 pages.

Office Action for U.S. Appl. No. 10/697,846 mailed Jan. 5, 2007, 16 pages.

Kruegal, Christopher, et al. "Using Decision Trees to Improve Signature-Based Intrusion Detection", Sep. 8, 2003, RAID 2003: recent Advance in Intrusion Detection, 20 pages.

Branch, Joel, et al., "Denial of Service Intrusion Detection Using Time Dependent Deterministic Finite Automata", RPI Graduate Research Conference 2002, Oct. 17, 2002, 7 pages.

Juniper Networks, "Attack Prevention," www.juniper.net/products/intrusion/prevention.html, downloaded Jun. 11, 2004, 2 pages.

Juniper Networks, "Attack Detection," www.juniper.net/products/intrusion/detection.html, downloaded Jun. 11, 2004, 7 pages.

Juniper Networks, "Intrusion Detection and Prevention," www.juniper.net/products/intrusion/downloaded Jun. 11, 2004, 2 pages.

Juniper Networks, "Architecture," www.juniper.net/products/intrusion/architecture.html, downloaded Jun. 11, 2004, 3 pages.

Juniper Networks, "Juniper Networks NetScreen-IDP 10/100/500/1000," Intrusion Detection and Prevention, Spec Sheet, Apr. 2004, 2 pages.

Roberts, Paul, "NetScreen Announces Deep Inspection Firewall," IDG News Service, Oct. 20, 2003, http://www.nwfusion.com/news/2003/1020netscannou.html, downloaded Jun. 11, 2004, 5 pages.

Snort.org, "The Open Source Network Intrusion Detection System", www.snort.org/about.html, 2 pages.

Blyth, Andrew, "Detecting Intrusion", School of Computing, University of Glamorgan, 14 pages.

Office Action mailed Mar. 1, 2010 for U.S. Appl. No. 11/112,252, filed Apr. 21, 2005., 40 pages.

Final Office Action mailed Oct. 19, 2009 for U.S. Appl. No. 11/112,252, filed Apr. 21, 2005., 32 pages.

Office Action mailed Mar. 31, 2009 for U.S. Appl. No. 11/112,252, filed Apr. 21, 2005., 35 pages.

Office Action mailed Apr. 29, 2008 of U.S. Appl. No. 11/112,252, filed Apr. 21, 2005. 25 pages.

Office Action mailed Nov. 14, 2008 of U.S. Appl. No. 11/112,252, filed Apr. 21, 2005. 26 pages.

Office Action mailed Oct. 2, 2007 of U.S. Appl. No. 10/964,871, filed Oct. 13, 2004. 19 pages.

Final Office Action mailed Mar. 20, 2008 of U.S. Appl. No. 10/964,871, Oct. 13, 2004. 19 pages.

Office Action mailed Jul. 16, 2008 of U.S. Appl. No. 10/964,871, Oct. 13, 2004. 21 pages.

Office Action mailed Jan. 9, 2009 of U.S. Appl. No. 10/964,871, Oct. 13, 2004. 21 pages.

"SonicWALL Content Filtering Service," Comprehensive Internet Security™, © 2005, 2pp.

SonicW ALL Internet Security Appliances, "Content Security Manager Integrated Solutions Guide", Version 3.0, © 2007, 160 pp.

SonicW ALL Internet Security Appliances, "SonicOS 3.8 Standard Administrator's Guide", © 2007, 362 pp.

"SonicOS Standard 3.8.0.2 Release Notes, SonicWALL Secure Anti-Virus Router 80 Series," SonicW ALL, Inc., Software Release: Apr. II, 2007, 13 pp.

Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service, Unified Threat Management, Intelligent Real-time Protection, © 2005 , 2 pp.

"SonicWALL Endpoint Security: Anti-Virus, Automated and Enforced Anti-Virus and Anti-Spyware Protection," © 2007, Mar. 2007, 2 pp.

"SonicWaLL Content Security Manager Series, Easy-to-use, Affordable, Content Security and Internet Threat Protection," © 2006, Dec. 2006, 4 pp.

"SonicWALL Complete Anti-Virus, Automated and Enforced Anti-Virus Protection," © 2005, 2 pp.

Aggarwal, N., "Improving the Efficiency of Network Intrusion Detection Systems", Indian Institue of Technology, May 3, 2006, pp. 1-40.

Van Engelen, R., "Constucting Finite State Automata for High-Performance XML Web Services," International Symposium on Web Services and Applications, 2004, pp. 1-7.

Lucas, Simon M., et al., "Learning Deterministic Finite Automata with a Smart State Labeling Evolutionary Algorithm," IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 27, No. 7, Jul. 2005, pp. 1063-1074.

Office Action mailed Jul. 7, 2010 of U.S. Appl. No. 11/778,546, Jul. 16, 2007. 15 pages.

Office Action mailed May 14, 2009 of U.S. Appl. No. 11/772,723, Jul. 2, 2007. 7 pages.

Office Action mailed Oct. 23, 2009 of U.S. Appl. No. 11/772,723, Jul. 2, 2007. 8 pages.

* cited by examiner

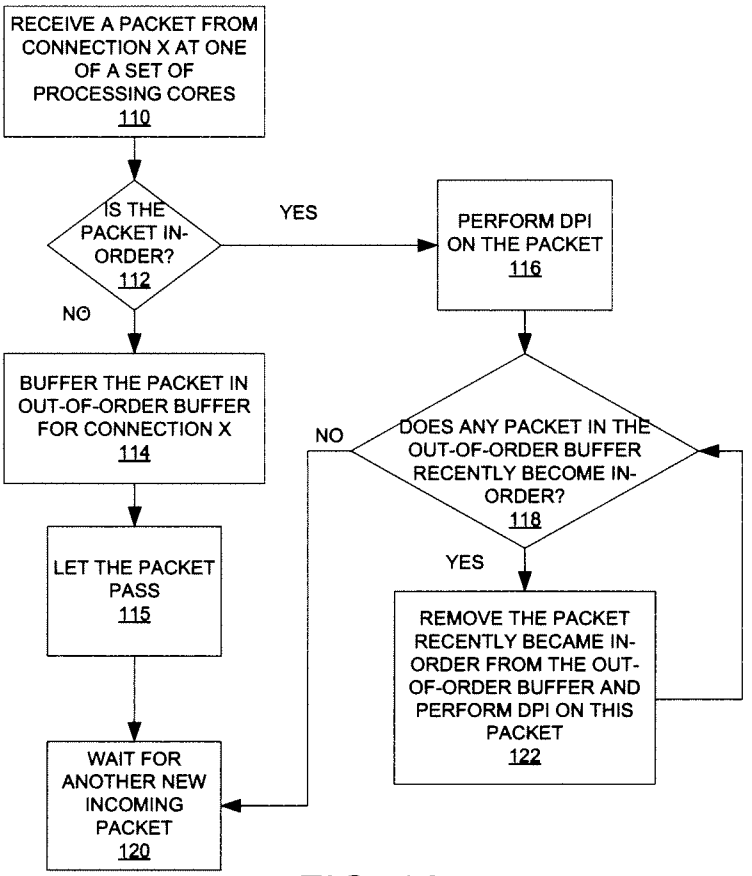

RECEIVE A PACKET FROM CONNECTION X AT ONE OF A SET OF PROCESSING CORES 110
IS THE PACKET IN-ORDER? 112
YES
NO
PERFORM DPI ON THE PACKET 116
BUFFER THE PACKET IN OUT-OF-ORDER BUFFER FOR CONNECTION X 114
DOES ANY PACKET IN THE OUT-OF-ORDER BUFFER RECENTLY BECOME IN-ORDER? 118
NO
YES
LET THE PACKET PASS 115
REMOVE THE PACKET RECENTLY BECAME IN-ORDER FROM THE OUT-OF-ORDER BUFFER AND PERFORM DPI ON THIS PACKET 122
WAIT FOR ANOTHER NEW INCOMING PACKET 120

FIG. 1A

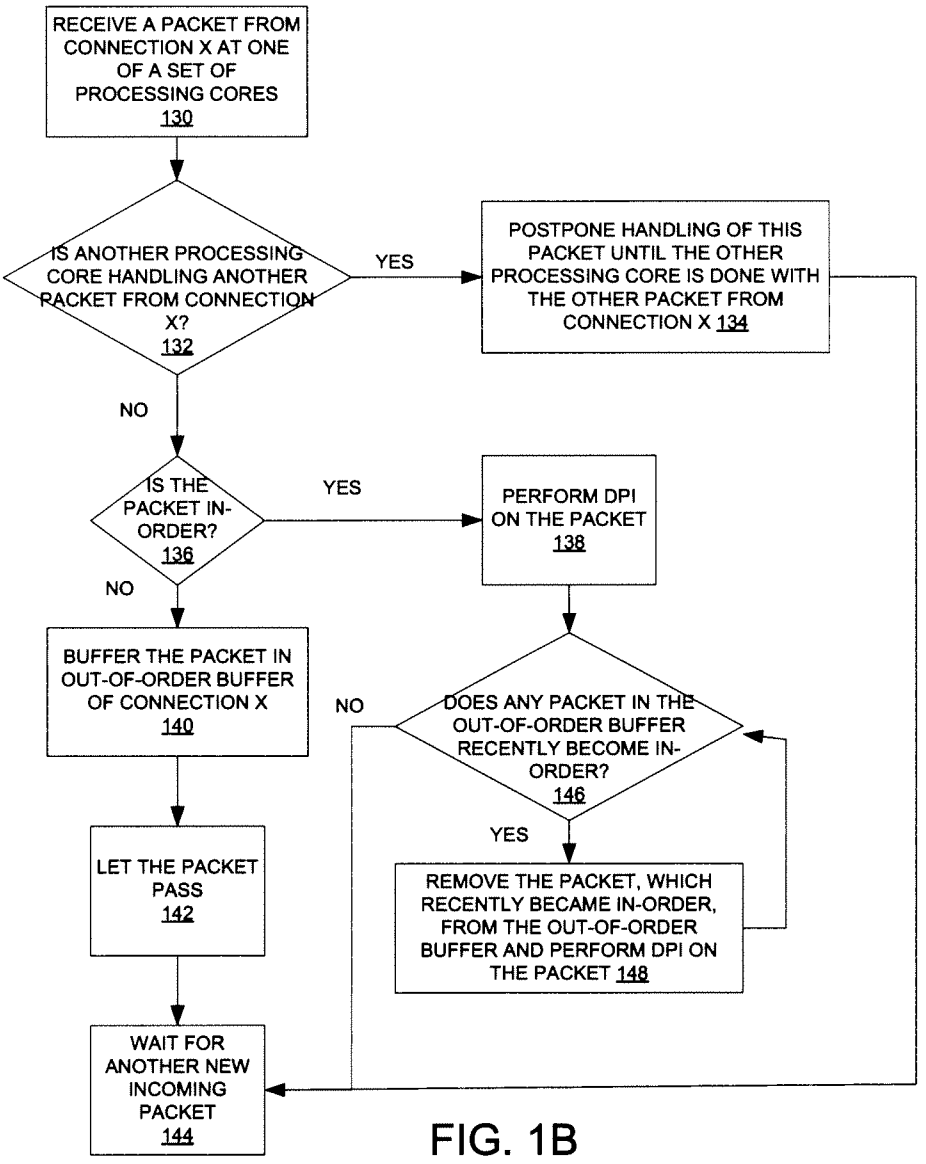

RECEIVE A PACKET FROM CONNECTION X AT ONE OF A SET OF PROCESSING CORES 130
IS ANOTHER PROCESSING CORE HANDLING ANOTHER PACKET FROM CONNECTION X? 132
YES
POSTPONE HANDLING OF THIS PACKET UNTIL THE OTHER PROCESSING CORE IS DONE WITH THE OTHER PACKET FROM CONNECTION X 134
NO
IS THE PACKET IN-ORDER? 136
YES
PERFORM DPI ON THE PACKET 138
NO
BUFFER THE PACKET IN OUT-OF-ORDER BUFFER OF CONNECTION X 140
NO
DOES ANY PACKET IN THE OUT-OF-ORDER BUFFER RECENTLY BECOME IN-ORDER? 146
YES
REMOVE THE PACKET, WHICH RECENTLY BECAME IN-ORDER, FROM THE OUT-OF-ORDER BUFFER AND PERFORM DPI ON THE PACKET 148
LET THE PACKET PASS 142
WAIT FOR ANOTHER NEW INCOMING PACKET 144

FIG. 1B

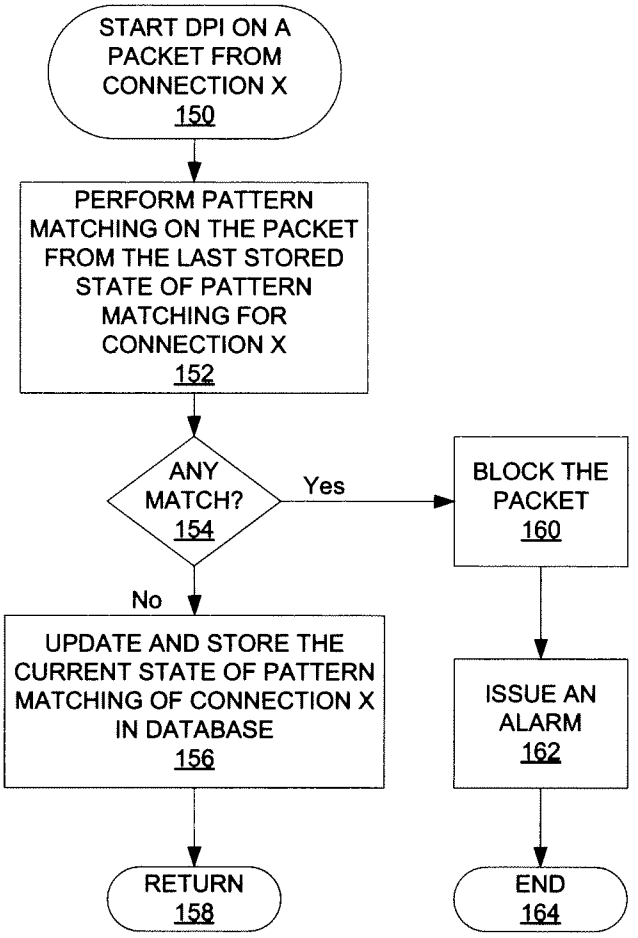

START DPI ON A PACKET FROM CONNECTION X
150
PERFORM PATTERN MATCHING ON THE PACKET FROM THE LAST STORED STATE OF PATTERN MATCHING FOR CONNECTION X
152
ANY MATCH?
154
Yes
BLOCK THE PACKET
160
No
UPDATE AND STORE THE CURRENT STATE OF PATTERN MATCHING OF CONNECTION X IN DATABASE
156
ISSUE AN ALARM
162
RETURN
158
END
164

Figure 1C

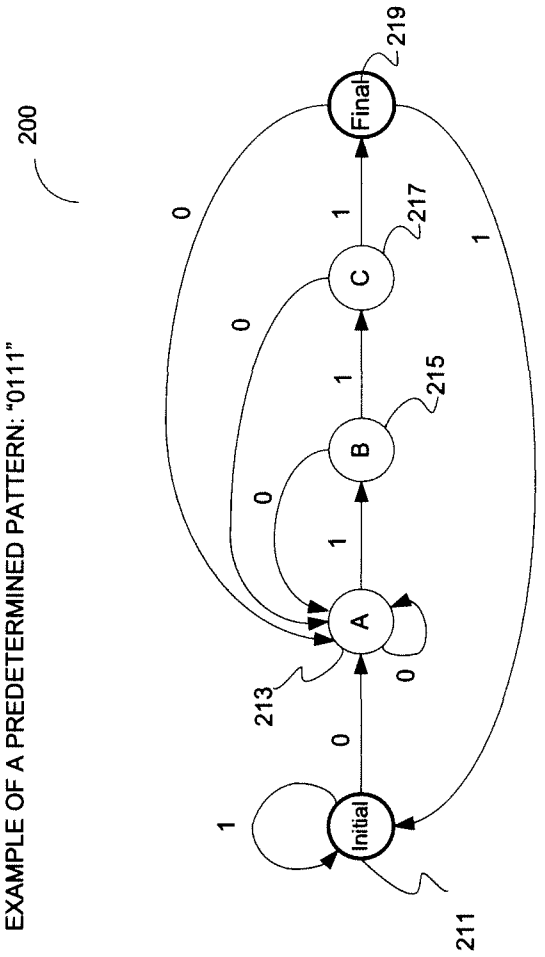

200
EXAMPLE OF A PREDETERMINED PATTERN: "0111"
Initial
A
B
C
Final
211
213
215
217
219
0
1
0
1
0
1
0
1
0
1

Figure 2

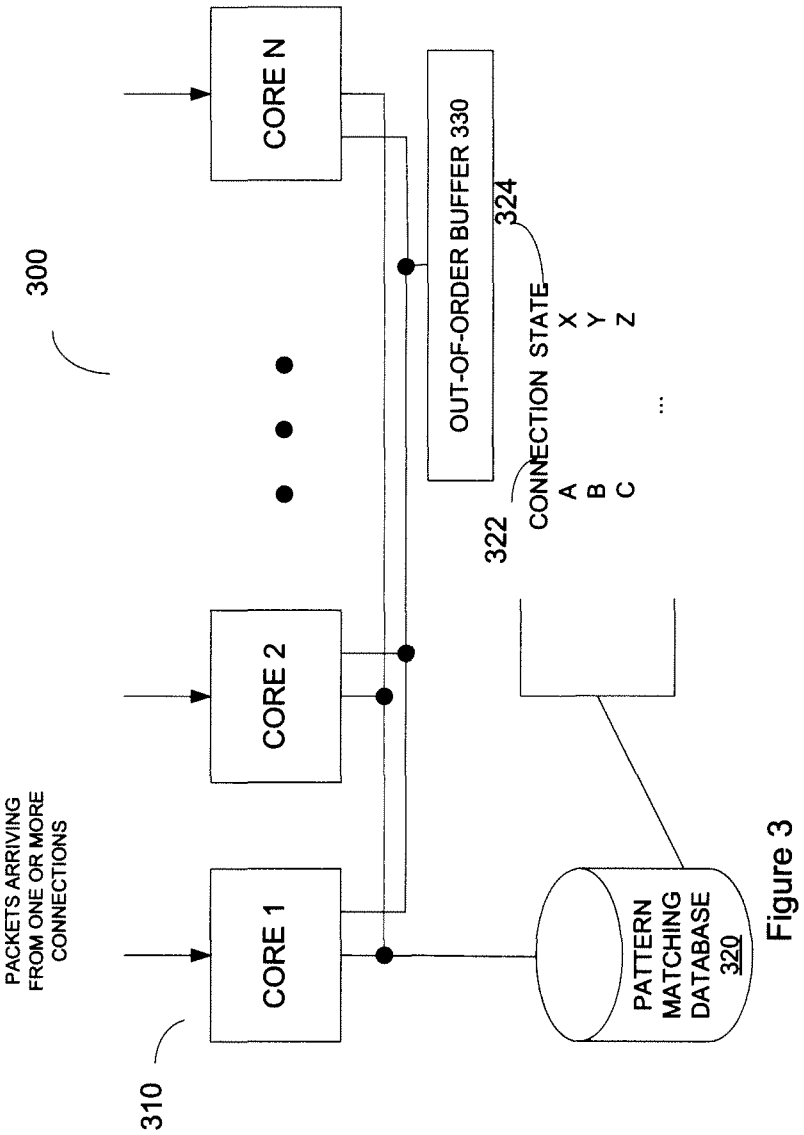

300
CORE N
CORE 2
CORE 1
310
PACKETS ARRIVING FROM ONE OR MORE CONNECTIONS
OUT-OF-ORDER BUFFER 330
324
CONNECTION STATE
322
A
B
C
X
Y
Z
...
PATTERN MATCHING DATABASE 320

Figure 3

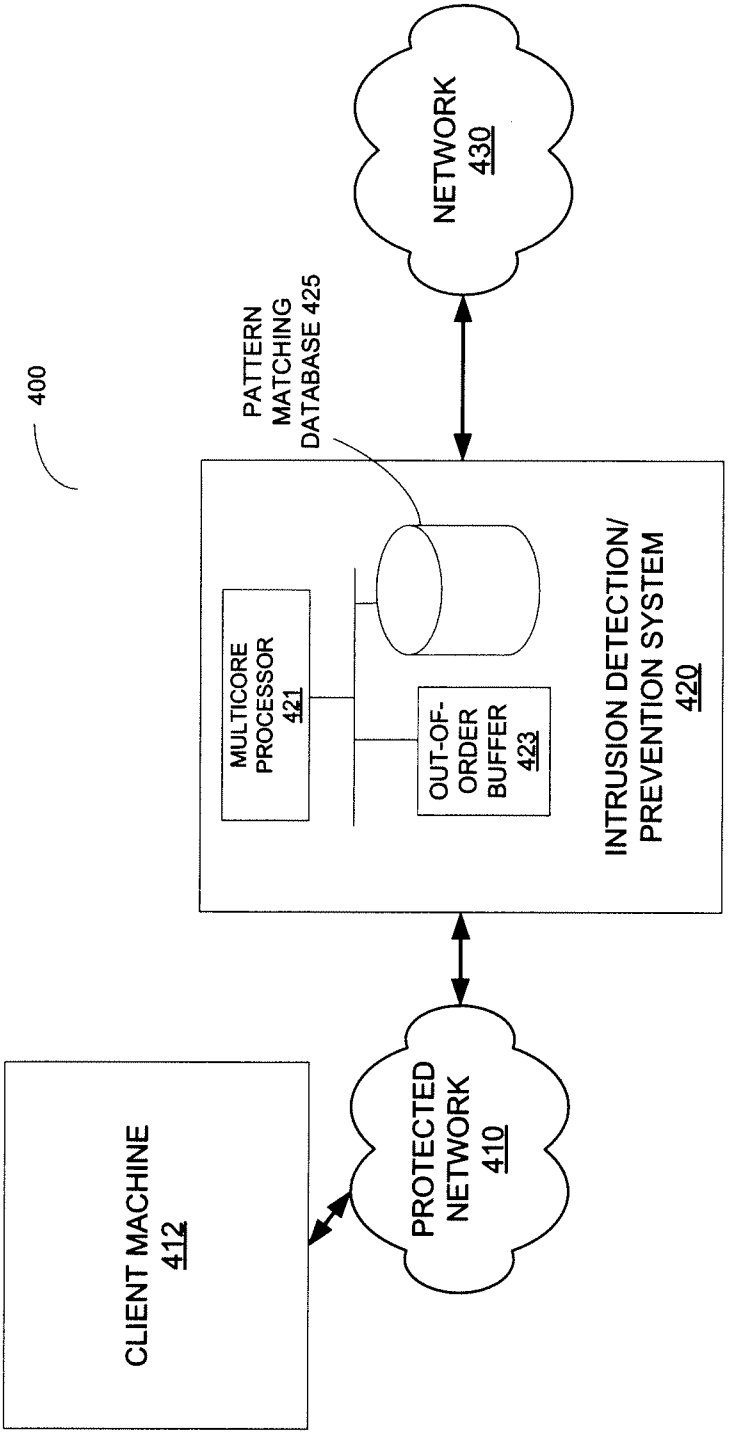

400
NETWORK
430
PATTERN
MATCHING
DATABASE 425
MULTICORE
PROCESSOR
421
OUT-OF-
ORDER
BUFFER
423
INTRUSION DETECTION/
PREVENTION SYSTEM
420
PROTECTED
NETWORK
410
CLIENT MACHINE
412

Figure 4

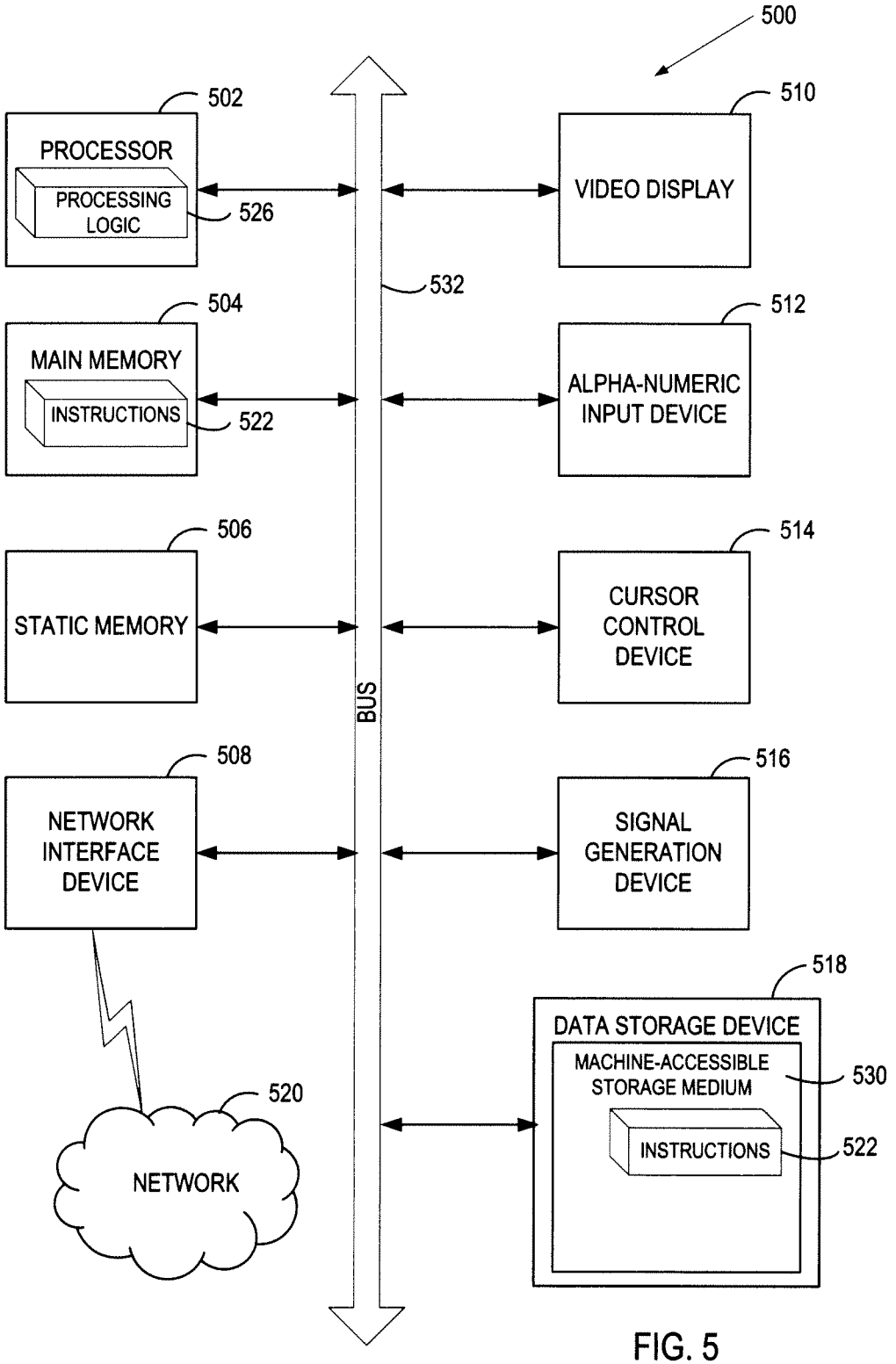

500
502
PROCESSOR
PROCESSING LOGIC
526
504
MAIN MEMORY
INSTRUCTIONS
522
506
STATIC MEMORY
508
NETWORK INTERFACE DEVICE
520
NETWORK
BUS
532
510
VIDEO DISPLAY
512
ALPHA-NUMERIC INPUT DEVICE
514
CURSOR CONTROL DEVICE
516
SIGNAL GENERATION DEVICE
518
DATA STORAGE DEVICE
MACHINE-ACCESSIBLE STORAGE MEDIUM
530
INSTRUCTIONS
522

FIG. 5

REASSEMBLY-FREE DEEP PACKET INSPECTION ON MULTI-CORE HARDWARE

TECHNICAL FIELD

The present invention relates to intrusion detection and prevention in a networked system, and more particularly, to performing multiple packet payloads analysis on multi-core hardware.

BACKGROUND

Today, in many security products, scanning by pattern matching is used to prevent many types of security attacks. For example, some existing desktop virus scanning may include scanning files against certain recognizable patterns. These files may come from mail attachments or website downloads. These desktop applications are simpler in that by the time the pattern matching is performed, the input has been all accumulated in the correct order. The situation is more complicated for gateway products, such as firewalls, attempting to match patterns for other purposes. Some of these products scan for patterns over Transport Control Protocol (TCP) packets. Since TCP usually breaks down application data into chunks called TCP segments, the full pattern may reside in several TCP segments. One conventional approach is to reassemble all TCP packets together into one large chunk and perform pattern matching on this chunk, similar to scanning files. The disadvantage of this approach is that this approach requires processing to reassemble, and it further requires memory to buffer the intermediate result before pattern matching can take place.

To further complicate the problem, many security attacks exhibit more than one pattern, and thus, multiple pattern matching has to be performed in order to successfully screen out these attacks. Such a collection of patterns is called a signature. For example, an attack signature may contain a recognizable header and a particular phrase in the body. To detect such an attack, the detection mechanism has to match all the patterns in the signature. If only part of the signature is matched, false positives may occur. As such, the term "attack pattern" is used to refer to a single pattern or a signature.

When such attacks are transported over TCP, the contents, and therefore the recognizable patterns, may exist in different TCP segments. In fact, even a single pattern is often split over several segments. Therefore, two problems have to be solved at the same time. On one hand, the detection mechanism has to scan each pattern across multiple segments, and on the other hand, the detection mechanism also has to scan across patterns. One existing approach is to reassemble all packets and scan for each pattern in sequence. This approach is inefficient in terms of processing time and memory usage because scanning cannot start until all packets are received and reassembled and extra memory is needed to store the packets received.

Another problem in pattern matching is that the packets may arrive out of order. Again, using TCP as an example, the application data is broken into what TCP considers the best sized chunks to send, called a TCP segment or a TCP packet. When TCP sends a segment, it maintains a timer and waits for the other end to acknowledge the receipt of the segment. The acknowledgement is commonly called an ACK. If an ACK is not received for a particular segment within a predetermined period of time, the segment is retransmitted. Since the IP layer transmits the TCP segments as IP datagrams and the IP datagrams can arrive out of order, the TCP segments can arrive out of order as well. Currently, one receiver of the TCP segments reassembles the data so that the application layer receives data in the correct order.

An existing Intrusion Detection/Prevention System (IPS) typically resides between the two ends of TCP communication, inspecting the packets as the packets arrive at the IPS. The IPS looks for predetermined patterns in the payloads of the packets. These patterns are typically application layer patterns. For example, the pattern might be to look for the word "windows." However, the word may be broken into two TCP segments, e.g., "win" in one segment and "dows" in another segment. If these two segments arrive in the correct order, then IPS can detect the word. However, if the segments arrive out of order, which happens relatively often, then the IPS may first receive the segment containing "dows", and have to hold this segment and wait for the other segment. A typical approach is for the IPS to force the sender to retransmit all the segments from the last missing one, hoping that the segments may arrive in order the second time. One disadvantage of this approach is the additional traffic in between and the additional processing on both ends of the TCP communication.

To take advantage of the introduction of multi-core processors (e.g., Intel® Core™2 Quad Processors from Intel Corporation of Santa Clara, Calif.), some conventional ISPs use multi-core processors to scan incoming segments to speed up the process. In general, each multi-core processor has two or more processing cores. According to one conventional approach, one of the processing cores is used to completely reassemble the file while the remaining processing cores perform scanning or pattern matching in the background after the file has been completely reassembled. However, this approach does not scale in terms of having enough memory to store all files. Also, background scanning by multiple processing cores is less efficient due to extra memory copying overhead and extra scheduling processing overhead.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings and in which:

FIG. **1**A illustrates one embodiment of a method to perform multiple packet analysis on multi-core hardware.

FIG. **1**B illustrates an alternate embodiment of a method to perform multiple packet analysis on multi-core hardware.

FIG. **1**C illustrates one embodiment of a method to perform deep packet inspection.

FIG. **2** illustrates an exemplary Deterministic Finite Automaton (DFA) according to one embodiment of the invention.

FIG. **3** illustrates a functional block diagram of one embodiment of multi-core hardware usable to perform multiple packet analysis.

FIG. **4** illustrates one embodiment of a system in which embodiments of the present invention may be implemented.

FIG. **5** illustrates a block diagram of an exemplary computer system, in accordance with one embodiment of the present invention.

DETAILED DESCRIPTION

Described herein are some embodiments of reassembly-free deep packet inspection on multi-core hardware. In one embodiment, a set of packets of one or more files is received at a networked device from one or more connections. Each packet is scanned using one of a set of processing cores in the

networked device without buffering the one or more files in the networked device. Furthermore, the set of processing cores may scan the packets substantially concurrently.

In the following description, numerous details are set forth. It will be apparent, however, to one skilled in the art, that the present invention may be practiced without these specific details. In some instances, well-known structures and devices are shown in block diagram form, rather than in detail, in order to avoid obscuring the present invention.

Some portions of the detailed descriptions below are presented in terms of algorithms and symbolic representations of operations on data bits within a computer memory. These algorithmic descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like.

It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the following discussion, it is appreciated that throughout the description, discussions utilizing terms such as "processing" or "computing" or "calculating" or "determining" or "displaying" or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

The present invention also relates to apparatus for performing the operations herein. This apparatus may be specially constructed for the required purposes, or it may comprise a general-purpose computer selectively activated or reconfigured by a computer program stored in the computer. Such a computer program may be stored in a computer-readable storage medium, such as, but is not limited to, any type of disk including floppy disks, optical disks, CD-ROMs, and magnetic-optical disks, read-only memories (ROMs), random access memories (RAMs), EPROMs, EEPROMs, flash memory, magnetic or optical cards, or any type of media suitable for storing electronic instructions, and each coupled to a computer system bus.

The algorithms and displays presented herein are not inherently related to any particular computer or other apparatus. Various general-purpose systems may be used with programs in accordance with the teachings herein, or it may prove convenient to construct more specialized apparatus to perform the required method steps. The required structure for a variety of these systems will appear from the description below. In addition, the present invention is not described with reference to any particular programming language. It will be appreciated that a variety of programming languages may be used to implement the teachings of the invention as described herein.

FIG. **1**A illustrates one embodiment of a method to perform multiple packet analysis on multi-core hardware, where multiple processing cores of a set of processing cores are allowed to handle packets from the same connection (hereinafter, "connection X"). In some embodiments, the set of processing cores includes processing cores of a multi-core processor. The method may be performed by processing logic that may comprise hardware (e.g., circuitry, dedicated logic, programmable logic, processing cores, etc.), software (such as instructions run on a processing core), firmware, or a combination thereof.

Initially, one of a set of processing cores receives a packet from connection X (processing block **110**). The packet is part of a file, which may be re-constructed by re-assembling the packet with other packets of the file. Then the processing core determines if the packet is in-order (processing block **112**). For example, the processing core may check a sequence number in a header of the packet against a next packet sequence number of connection X, which may be stored in a database commonly accessible by the processing cores.

If the packet is not in-order, i.e., out-of-order, then the processing core may buffer the packet in an out-of-order buffer associated with connection X (processing block **114**). The processing core may allow the packet to pass (processing block **115**). Then the processing core waits for another new incoming packet (processing block **120**).

If the packet is in-order, then the processing core performs deep packet inspection (DPI) on the packet (processing block **116**). Details of some embodiments of DPI are discussed below. Then the processing core checks if there is any packet in the out-of-order buffer associated with connection X that recently became in-order (processing block **118**). If there is no packet in the out-of-order buffer associated with connection X that is next in sequence (in-order), the processing core transitions to processing block **120** to wait for another new incoming packet. Otherwise, if there is a packet in the out-of-order buffer associated with connection X that is now in-order, then the processing core removes this packet and performs DPI on this packet (processing block **122**). When the processing core completes DPI on this packet, the processing core returns to processing block **118** to check if there is another packet in the out-of-order buffer associated with connection X that is in-order.

Note that the incoming packets are scanned without buffering the file for reassembly because the packets can be inspected for the predetermined pattern without being reassembled into the file. Thus, the above technique is well suited for IPSs that have limited capacity for buffering or storage. Furthermore, the above technique allows the set of processing cores to scan incoming packets substantially concurrently. Therefore, the speed of the scanning may be improved over conventional approaches.

FIG. **1**B illustrates one embodiment of a method to perform multiple payload analysis on multi-core hardware, where only a single core in a set of processing cores is allowed to handle packets from a particular connection (hereinafter, "connection X") at a time. In some embodiments, the set of processing cores includes processing cores of a multi-core processor. The method may be performed by processing logic that may comprise hardware (e.g., circuitry, dedicated logic, programmable logic, processing cores, etc.), software (such as instructions run on a processing core), firmware, or a combination thereof.

Initially, one processing core of the set of processing cores receives a packet from connection X (processing block **130**). Then the processing core checks if there is another processing core in the set of processing cores handling another packet from connection X (processing block **132**). If there is another processing core handling another packet from connection X

currently, then the processing core postpones handling of this packet until the other processing core is done with the other packet from connection X (processing block **134**). The processing core may transition to processing block **144** to wait for another new incoming packet.

If the processing core determines that there is no other processing core in the set of processing cores handling another packet from connection X, then the processing core checks if this packet is in-order (processing block **136**). If this packet is not in-order, i.e., out-of-order, then the processing core buffers this packet in an out-of-order buffer associated with connection X (processing block **140**). The processing core may allow this packet to pass (processing block **142**). Then the processing core waits for another new incoming packet (processing block **144**).

If the processing core determines that this packet is in-order, then the processing core performs DPI on this packet (processing block **138**). Details of some embodiments of DPI are discussed below. After performing DPI on the packet, the processing core checks if there is any packet in the out-of-order buffer associated with connection X, which is now in-order (processing block **146**). If there is a packet in the out-of-order buffer that is now in-order, then the processing core removes the packet that recently became in-order from the out-of-order buffer and performs DPI on this packet (processing block **148**). Then the processing core returns to processing block **146** to repeat the above process. If there is no packet in the out-of-order buffer that is in-order, then the processing core transitions to processing block **144** to wait for another new incoming packet.

Like the technique illustrated in FIG. **1**A, the technique illustrated in FIG. **1**B also allows scanning of the incoming packets without buffering the file for reassembly because the packets can be scanned for the predetermined pattern, without reassembling the packets into the file, by DPI.

FIG. **1**C illustrates one embodiment of a method to perform deep packet inspection (DPI) using one of a set of processing cores. In some embodiments, the set of processing cores includes processing cores of a multi-core processor. The method may be performed by processing logic that may comprise hardware (e.g., circuitry, dedicated logic, programmable logic, processing cores, etc.), software (such as instructions run on a processing core), firmware, or a combination thereof.

Initially, the processing core starts DPI on a packet from connection X at block **150**. This packet is hereinafter referred to as the current packet. The processing core performs pattern matching on the current packet from the last stored state of pattern matching for connection X (processing block **152**). Specifically, the processing core is trying to look for a predetermined pattern or signature in the incoming packets, which may be associated with a computer virus or malicious code. By identifying such pattern or signature in the incoming packets and blocking at least one of the packets containing part of the predetermined pattern or signature, the set of processing cores can protect a system from computer viral attack. In some embodiments, the last stored state of pattern matching for connection X is stored in a database commonly accessible by the set of processing cores. As such, each of the set of processing cores can handle packets from connection X, even though some of the packets may be inspected by different processing cores.

In some embodiments, if there is a match between a predetermined pattern and the data pattern in the incoming packets inspected so far (which includes the current packet), then the processing core blocks the current packet (processing block **160**). Then the processing core may issue an alarm to warn a system administrator of detection of potentially malicious code or virus in the incoming packets (processing block **162**), and the process ends at block **164**.

If there is no match between the predetermined pattern and the data pattern in the incoming packets inspected so far, then the processing core may update and store the current state of pattern matching of connection X in the database (processing block **156**). The method then ends at block **158**.

In some embodiments, pattern matching performed in DPI is accomplished using Deterministic Finite Automaton (DFA). An exemplary DFA is shown in FIG. **2** to illustrate the concept.

FIG. **2** illustrates an exemplary DFA according to one embodiment of the invention. In this example, an IPS is programmed to detect and to prevent a pattern of "0111" to pass through. The DFA **200** shown in FIG. **2** corresponds to this pattern. A set of processing cores may use the DFA **200** to perform pattern matching on a number of packets to determine whether the packets contain the pattern "0111". Furthermore, to simplify the illustration, it is assumed in this example that each packet contains only one digit. However, it should be appreciated that the concept is applicable to scenarios where a packet contains more than one digits and/or alphabetic letters.

Referring to FIG. **2**, the DFA **200** includes 5 states **211**-**219**. The states **211**-**219** in the DFA **200** may be referred to as nodes. A processing core in the set of processing cores begins pattern matching at the initial state **211**. If a packet received contains a "1", the processing core remains in the initial state **211**. If the packet contains a "0", which corresponds to the first digit in the predetermined pattern, the processing core transitions to the A state **213**.

If the processing core receives a "0" subsequently, the processing core remains in the A state **213**. If the processing core receives a "1", which corresponds to the second digit in the predetermined pattern, then the processing core transitions into the B state **215**. From the B state **215**, the processing core may transition back to the A state **213** if the next packet received contains a "0". If the next packet received contains a "1", which corresponds to the third digit in the predetermined pattern, then the processing core transitions to the C state **217**. However, note that another processing core in the set of processing cores may receive and process the next packet in some embodiments.

From the C state **217**, the processing core may transition back to the A state **213** if the next packet received contains a "0". If the next packet received contains a "1", which corresponds to the last digit in the predetermined pattern, then the processing core transitions to the final state **219**. When the processing core reaches the final state **219**, the processing core knows that the packets received so far contain the predetermined pattern. Hence, the processing core may perform the appropriate operations in response to receiving the predetermined pattern, such as blocking the packet of the predetermined pattern last received and issuing an alarm to alert system administrators. To keep track of which state of the DFA is in currently, the processing core stores the current state of the DFA in a database commonly accessible by the set of processing cores. As such, another processing core may continue pattern matching on the next packet from the current state if the other processing core receives the next packet. Furthermore, the current state of the DFA may be associated with a connection from which the packet is received so that the set of processing cores may inspect packets from multiple connections using the information from the database.

One advantage of using the DFA to perform pattern matching on packets is to eliminate the need to reassemble the

packets because the processing cores can walk through the DFA as each packet is received and examined. Because a pattern is typically broken up into a number of segments and each segment is transmitted using a packet, it is necessary to inspect multiple packets in order to identify the pattern. Using the DFA, the processing cores may not have to reassemble the packets in order to find out what the pattern contained in the packets is in order to match the pattern against a predetermined pattern. The processing cores may perform pattern matching on a packet-by-packet basis as each of the packets is received without reassembling the packets by walking through the DFA. If a processing core reaches a final state, there is a match between the pattern contained in the packets received so far and the predetermined pattern. There is no need to store the packets for reassembling the packets. Instead, the processing cores may simply store the current state of the DFA in a database commonly accessible by the processing cores.

The concept described above may be expanded to signature detection. A signature is a collection of multiple patterns. To keep track of which pattern within a signature is being matched, processing logic may use a tree structure, where each node within the tree structure corresponds to a pattern and each pattern is represented using a DFA. Alternatively, a single DFA may represent multiple patterns.

FIG. **3** illustrates a functional block diagram of one embodiment of multi-core hardware usable to perform multiple payload analysis in an IPS. The IPS may be implemented within a set-top box coupled to a protected network. The multi-core hardware **300** includes a set of processing cores **310**, a pattern matching database **320**, and an out-of-order buffer **330**. In some embodiments, the set of processing cores **310** includes processing cores in a multi-core processor. The processing cores **310** are communicably coupled to the database **320** so that each of the processing cores **310** may retrieve and update information in the database **320**. Likewise, the processing cores **310** are also communicably coupled to the out-of-order buffer **330** so that each of the processing cores **310** may access the out-of-order buffer **330**.

In some embodiments, the processing cores **310** receive packets from one or more connections. To prevent harmful virus or malicious code from reaching the protected network, the processing cores **310** performs reassembly-free DPI on the packets. When one of the processing cores **310** receives a packet, the processing core may determine if the packet is in-order or out-of-order. An out-of-order packet may be temporarily stored in the out-of-order buffer **330** and be associated with the connection from which the out-of-order packet is received. In-order packets are examined by the processing cores **310** and are allowed to pass to the protected network if no pattern of harmful virus or malicious code is detected. The processing cores **310** update and store the current pattern matching state of each connection in the database **320**. As such, any one of the processing cores **310** can continue with the on-going pattern matching from the current state of a connection that sends the current packet. In some embodiments, the database **320** includes a relational database that stores the current pattern matching states **324** with their corresponding connections **322** as shown in FIG. **2**. Details of some embodiments of the method to perform reassembly-free DPI have been discussed above.

FIG. **4** illustrates one embodiment of a system in which embodiments of the present invention may be implemented. The system **400** includes a client machine **412** within a protected network **410**, an IPS **420**, and a network **430**. The protected network **410** is communicably coupled to the network **430** via the IPS **420**. Thus, packets transmitting between the protected network **410** and the network **430** have to pass through the IPS **420**. In some embodiments, there may be more than one client machines coupled to the protected network **410**. The network **430** may include a variety of networks, such as local area network (LAN), wide area network (WAN), etc. Furthermore, the network **430** may be publicly accessible, and therefore, computer virus and malicious code targeting the protected network **410** may be sent from the network **430**. As such, the IPS **420** scans the incoming packets to prevent computer virus and malicious code from entering the protected network **410**.

In some embodiments, the IPS **420** includes a multi-core processor **421**, an out-of-order buffer **423**, and a pattern matching database **425**. The multi-core processor **421** includes a set of processing cores, such as the processing cores **310** shown in FIG. **3**.

In some embodiments, each of the processing cores receives packets from the network **430** through different connections. Furthermore, the packets may arrive out-of-order, and if so, the out-of-order packets may be temporarily stored in the out-of-order buffer **423** to be inspected later. The processing cores of the multi-core processor **421** perform DPI on the in-order packets and store the current pattern matching states of the connections in the pattern matching database **425**. If a pattern associated with computer virus or malicious code is identified in the incoming packets inspected so far, the multi-core processor **421** blocks the packet currently being inspected and may further issue a warning to a system administrator. If no pattern associated with computer virus or malicious code is identified in the incoming packets inspected so far, then the multi-core processor **421** allows the packet currently being inspected to pass to the protected network **410**, which may be further transmitted to the client machine **412**. By blocking the packet currently being inspected if the pattern is identified in the packets received so far, the computer virus or malicious code cannot be completely passed into the protected network **410**, and hence, the computer virus or malicious code cannot be completely reassembled on the client machine **412**. The incomplete computer virus or malicious code typically cannot harm the client machine **412** coupled thereto. Details of some embodiments of a method to perform reassembly-free DPI have been discussed above.

FIG. **5** illustrates a diagrammatic representation of a machine in the exemplary form of a computer system **500** within which a set of instructions, for causing the machine to perform any one or more of the methodologies discussed herein, may be executed. In alternative embodiments, the machine may be connected (e.g., networked) to other machines in a LAN, an intranet, an extranet, and/or the Internet. The machine may operate in the capacity of a server or a client machine in client-server network environment, or as a peer machine in a peer-to-peer (or distributed) network environment. The machine may be a personal computer (PC), a tablet PC, a set-top box (STB), a Personal Digital Assistant (PDA), a cellular telephone, a web appliance, a server, a network router, a switch or bridge, or any machine capable of executing a set of instructions (sequential or otherwise) that specify actions to be taken by that machine. Further, while only a single machine is illustrated, the term "machine" shall also be taken to include any collection of machines that individually or jointly execute a set (or multiple sets) of instructions to perform any one or more of the methodologies discussed herein.

The exemplary computer system **500** includes a processing device **502**, a main memory **504** (e.g., read-only memory (ROM), flash memory, dynamic random access memory (DRAM) such as synchronous DRAM (SDRAM) or Rambus

DRAM (RDRAM), etc.), a static memory **506** (e.g., flash memory, static random access memory (SRAM), etc.), and a data storage device **518**, which communicate with each other via a bus **532**.

Processing device **502** represents one or more general-purpose processing devices such as a microprocessor, a central processing unit, or the like. More particularly, the processing device may be complex instruction set computing (CISC) microprocessor, reduced instruction set computing (RISC) microprocessor, very long instruction word (VLIW) microprocessor, or processor implementing other instruction sets, or processors implementing a combination of instruction sets. Processing device **502** may also be one or more special-purpose processing devices such as an application specific integrated circuit (ASIC), a field programmable gate array (FPGA), a digital signal processor (DSP), network processor, or the like. The processing device **502** is configured to execute the processing logic **526** for performing the operations and steps discussed herein.

The computer system **500** may further include a network interface device **508**. The computer system **500** also may include a video display unit **510** (e.g., a liquid crystal display (LCD) or a cathode ray tube (CRT)), an alphanumeric input device **512** (e.g., a keyboard), a cursor control device **514** (e.g., a mouse), and a signal generation device **516** (e.g., a speaker).

The data storage device **518** may include a machine-accessible storage medium **530** (also known as a machine-readable storage medium or a computer-readable medium) on which is stored one or more sets of instructions (e.g., software **522**) embodying any one or more of the methodologies or functions described herein. The software **522** may also reside, completely or at least partially, within the main memory **404** and/or within the processing device **502** during execution thereof by the computer system **500**, the main memory **504** and the processing device **502** also constituting machine-accessible storage media. The software **522** may further be transmitted or received over a network **520** via the network interface device **508**.

While the machine-accessible storage medium **530** is shown in an exemplary embodiment to be a single medium, the term "machine-accessible storage medium" should be taken to include a single medium or multiple media (e.g., a centralized or distributed database, and/or associated caches and servers) that store the one or more sets of instructions. The term "machine-accessible storage medium" shall also be taken to include any medium that is capable of storing, encoding or carrying a set of instructions for execution by the machine and that cause the machine to perform any one or more of the methodologies of the present invention. The term "machine-accessible storage medium" shall accordingly be taken to include, but not be limited to, solid-state memories, optical and magnetic media, etc. In some embodiments, machine-accessible storage medium may also be referred to as computer-readable storage medium.

Thus, some embodiments of reassembly-free DPI on multi-core hardware have been described. It is to be understood that the above description is intended to be illustrative, and not restrictive. Many other embodiments will be apparent to those of skill in the art upon reading and understanding the above description. The scope of the invention should, therefore, be determined with reference to the appended claims, along with the full scope of equivalents to which such claims are entitled.

What is claimed is:

1. A method comprising:

receiving a plurality of packets of one or more files at a networked device comprising a plurality of processing cores, the packets from a plurality of connections;

processing each of the received packets, wherein processing each received packet comprises:

determining from which of the plurality of connections the packet came, and

postponing processing one of the received packets based on a determination that another processing core is currently processing a packet from a same connection, and

continuing to process the one of the received packets based on a determination that no other processing core is currently processing a packet from the same connection;

storing a current state of pattern matching in a database in memory accessible to each of the plurality of processing cores, wherein the current state of pattern matching corresponds to packets received from the determined corresponding connection, and wherein a plurality of other current states of pattern matching are stored for other connections from the plurality of connections;

scanning each of the plurality of packets using one of the plurality of processing cores in the networked device without buffering the one or more files in the networked device, such that the plurality of processing cores scan the plurality of packets substantially concurrently, wherein when the plurality of packets are from one of the plurality of connections, a first processing core of the plurality of processing core receives an in-order packet and scans the in-order packet, a second processing core of the plurality of processing core receives an out-of-order packet and temporarily buffers the out-of-order packet in an out-of-order buffer without scanning the out-of-order packet, wherein the first processing core retrieves a next in order packet from the out-of-order buffer to scan after scanning the in-order packet; and

updating the current state of pattern matching based on a plurality of scan results from the plurality of processing cores, the updated current state of pattern matching stored with the determined corresponding connection.

2. The method of claim **1**, further comprising: resolving conflicts between out-of-order packets among the plurality of packets.

3. The method of claim **2**, wherein when the plurality of packets are from distinct ones of the plurality of connections, the first processing core of the plurality of processing cores receives a first packet from a first connection, and resolving conflicts between out-of-order packets further comprises:

the first processing core determining if the first packet is in-order or out-of order;

the first processing core scanning the packet if the first packet is in-order; and

the first processing core temporarily buffering the first packet in an out-of order buffer associated with the first connection without scanning the first packet if the first packet is out-of-order.

4. The method of claim **3**, wherein resolving conflicts between out-of-order packets further comprises:

the second processing core of the plurality of processing cores receiving a second packet from the first connection while the first processing core is still processing the first packet; and

the second processing core re-scheduling scanning of the second packet to a later time.

5. The method of claim 1, wherein storing the current state of pattern matching further comprises storing a plurality of current states in the database, each current state associated with one of the plurality of connections.

6. An apparatus comprising:

a network interface to receive a plurality of packets of one or more files from a plurality of connections;

a plurality of processing cores to perform reassembly-free deep packet inspection on the plurality of packets without buffering the one or more files such that the plurality of processing cores scan the plurality of packets substantially concurrently, wherein each processing core processes each received packet by:

determining from which of the plurality of connections the packet came,

postponing processing one of the received packets based on a determination that another processing core is currently processing a packet from a same connection, and

continuing to process the one of the received packets based on a determination that no other processing core is currently processing a packet from the same connection, wherein when the plurality of packets are from one of the plurality of connections, a first processing core of the plurality of processing core receives an in-order packet and scans the in-order packet, a second processing core of the plurality of processing core receives an out-of-order packet and temporarily buffers the out-of-order packet in an out-of-order buffer without scanning the out-of-order packet, wherein the first processing core retrieves a next in order packet from the out-of-order buffer to scan after scanning the in-order packet; and

memory accessible to each of the plurality of processing cores, the memory associated with a database for storing a current state of pattern matching, the current state of pattern matching corresponding to packets from the determined corresponding connection, wherein a plurality of other current states of pattern matching are stored for other connections from the plurality of connections, wherein the current state of pattern matching is updated based on a plurality of scan results from the plurality of processing cores, the updated current state of pattern matching stored with the determined corresponding connection.

7. The apparatus of claim 6, wherein the plurality of processing cores resolve conflicts between out-of-order packets among the plurality of packets.

8. The apparatus of claim 6, wherein when the plurality of packets are from distinct ones of the plurality of connections, the first processing core of the plurality of processing cores receives a first packet from a first connection and scans the packet if the first packet is in-order, and temporarily buffers the first packet in an out-of-order buffer associated with the first connection without scanning the first packet if the first packet is out-of-order.

9. The apparatus of claim 6, wherein the second processing core to receive a second packet from a first connection while the first processing core is still processing the first packet, and to re-schedule scanning of the second packet to a later time.

10. The apparatus of claim 6, wherein the database further stores a plurality of current states, each current state associated with one of the plurality of connections.

11. A system comprising the apparatus of claim 6, further comprising: one or more client devices coupled to receive the plurality of packets after the plurality of packets have been scanned without identifying any prohibited content.

12. A non-transitory computer-readable medium embodying instructions that, when executed by a processor, will cause the processor to perform operations comprising:

receiving a plurality of packets of one or more files at a networked device comprising a plurality of processing cores, the packets from plurality of connections;

processing each of the received packets, wherein processing each received packet comprises:

determining from which of the plurality of connections the packet came,

postponing processing one of the received packets based on a determination that another processing core is currently processing a packet from a same connection, and

continuing to process the one of the received packets based on a determination that no other processing core is currently processing a packet from the same connection;

storing a current state of pattern matching in a database accessible to each of the plurality of processing cores, wherein the current state of pattern matching corresponds to packets from the determined corresponding connection, and wherein a plurality of other current states of pattern matching are stored for other connections from the plurality of connections;

scanning each of the plurality of packets using one of the plurality of processing cores in the networked device without buffering the one or more files in the networked device, such that the plurality of processing cores scan the plurality of packets substantially concurrently, wherein when the plurality of packets are from one of the plurality of connections, a first processing core of the plurality of processing core receives an in-order packet and scans the in-order packet, a second processing core of the plurality of processing core receives an out-of-order packet and temporarily buffers the out-of-order packet in an out-of-order buffer without scanning the out-of-order packet, wherein the first processing core retrieves a next in order packet from the out-of-order buffer to scan after scanning the in-order packet; and

updating the current state of pattern matching based on a plurality of scan results from the plurality of processing cores, the updated current state of pattern matching stored with the determined corresponding connection.

13. The non-transitory computer-readable medium of claim 12, wherein the operations further comprise: resolving conflicts between out-of-order packets among the plurality of packets.

14. The non-transitory computer-readable medium of claim 12, wherein when the plurality of packets are from distinct ones of the plurality of connections, the first processing core of the plurality of processing cores receives a first packet from a first connection, and resolving conflicts between out-of-order packets further comprises:

the first processing core determining if the first packet is in-order or out-of order;

the first processing core scanning the packet if the first packet is in-order; and

the first processing core temporarily buffering the first packet in an out-of order buffer associated with the first connection without scanning the first packet if the first packet is out-of-order.

15. The non-transitory computer-readable medium of claim 14, wherein resolving conflicts between out-of-order packets further comprises:

the second processing core of the plurality of processing cores receiving a second packet from the first connection while the first processing core is still processing the first packet; and

the second processing core re-scheduling scanning of the second packet to a later time.

16. The non-transitory computer-readable medium of claim **12**, wherein storing the current state of pattern matching further comprises: storing a plurality of current states in the database, each current state associated with one of the plurality of connections.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 8,813,221 B1
APPLICATION NO. : 12/238205
DATED : August 19, 2014
INVENTOR(S) : Dubrovsky et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the Claims

Column 10, Lines 44-46 should read:

2. The method of claim 1, further comprising[[:]] resolving conflicts between out-of-order packets among the plurality of packets.

Column 10, Lines 47-59 should read:

3. The method of claim 2, wherein when the plurality of packets are from distinct ones of the plurality of connections, the first processing core of the plurality of processing cores receives a first packet from a first connection, and resolving conflicts between out-of-order packets further comprises:

the first processing core determining if the first packet is in-order; and

the first processing core scanning the packet if the first packet is in-order.

Column 11, Lines 49-56 should read:

8. The apparatus of claim 6, wherein when the plurality of packets are from distinct ones of the plurality of connections, the first processing core of the plurality of processing cores receives a first packet from a first connection and scans the packet if the first packet is in-order.

Column 11, Lines 64-67 should read:

11. A system comprising the apparatus of claim 6, further comprising [[:]] one or more client devices coupled to receive the plurality of packets after the plurality of packets have been scanned without identifying any prohibited content.

Column 12, Lines 47-50 should read:

Signed and Sealed this
Eighteenth Day of August, 2015

Michelle K. Lee

Michelle K. Lee
Director of the United States Patent and Trademark Office

CERTIFICATE OF CORRECTION (continued)
U.S. Pat. No. 8,813,221 B1

13. The non-transitory computer-readable medium of claim 12, wherein the operations further comprise [[:]] resolving conflicts between out-of-order packets among the plurality of packets.

Column 12, Lines 51-64 should read:

14. The non-transitory computer-readable medium of claim [[12]] 13, wherein when the plurality of packets are from distinct ones of the plurality of connections, the first processing core of the plurality of processing cores receives a first packet from a first connection, and resolving conflicts between out-of-order packets further comprises:

the first processing core determining if the first packet is in-order; and

the first processing core scanning the packet if the first packet is in-order.

Column 13, Lines 7-11 should read:

16. The non-transitory computer-readable medium of claim 12, wherein storing the current state of pattern matching further comprises [[:]] storing a plurality of current states in the database, each current state associated with one of the plurality of connections.

Column 13, Lines 12-19 should read:

17. The method of claim 2, wherein when the plurality of packets are from distinct ones of the plurality of connections, the first processing core of the plurality of processing cores receives a first packet from a first connection, and resolving conflicts between out-of-order packets further comprises:

the first processing core determining if the first packet is out-of-order; and

the first processing core temporarily buffering the first packet in an out-of-order buffer associated with the first connection without scanning the first packet if the first packet is out-of-order.

Column 13, Lines 20-24 should read:

18. The apparatus of claim 6, wherein when the plurality of packets are from distinct ones of the plurality of connections, the first processing core of the plurality of processing cores receives a first packet from a first connection and temporarily buffers the first packet in an out-of-order buffer associated with the first connection without scanning the first packet if the first packet is out-of-order.

Column 13, Lines 25-32 should read:

19. The non-transitory computer-readable medium of claim 13, wherein when the plurality of packets

CERTIFICATE OF CORRECTION (continued)
U.S. Pat. No. 8,813,221 B1

are from distinct ones of the plurality of connections, the first processing core of the plurality of processing cores receives a first packet from a first connection, and resolving conflicts between out-of-order packets further comprises:

the first processing core determining if the first packet is out-of order; and

the first processing core temporarily buffering the first packet in an out-of order buffer associated with the first connection without scanning the first packet if the first packet is out-of-order.

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix X

This document was also filed as ECF No. 168-49 and can be found in this Joint Appendix at JA3404.

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix Y

This document was also filed as ECF No. 168-24 and can be found in this Joint Appendix at JA2748.

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix Z

This document was also filed as ECF No. 178-5 and can be found in this Joint Appendix at JA3728.

No. 20-1191

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

WIKIMEDIA FOUNDATION,

Plaintiff–Appellant,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants–Appellees.

On Appeal from the United States District Court
for the District of Maryland at Baltimore

JOINT APPENDIX—VOLUME 3 OF 7 (JA1791–JA2352)

H. Thomas Byron III
Joseph Busa
Michael Shih
U.S. DEPARTMENT OF JUSTICE
950 Pennsylvania Ave. NW
Washington, DC 20530
Phone: (202) 616-5367
Fax: (202) 307-2551
h.thomas.byron@usdoj.gov

Counsel for Defendants–Appellees

Patrick Toomey
Ashley Gorski
Charles Hogle
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
ptoomey@aclu.org

Counsel for Plaintiff–Appellant
(Additional counsel on next page)

Alex Abdo
Jameel Jaffer
KNIGHT FIRST AMENDMENT INSTITUTE AT COLUMBIA UNIVERSITY
475 Riverside Drive, Suite 302
New York, NY 10115
Phone: (646) 745-8500
alex.abdo@knightcolumbia.org

Deborah A. Jeon
David R. Rocah
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND
3600 Clipper Mill Rd., #350
Baltimore, MD 21211
Phone: (410) 889-8555
Fax: (410) 366-7838
rocah@aclu-md.org

Benjamin H. Kleine
COOLEY LLP
101 California Street, 5th Floor
San Francisco, CA 94111
Phone: (415) 693-2000
Fax: (415) 693-2222
bkleine@cooley.com

***Wikimedia Foundation v. National Security Agency, et al.*,**
No. 20-1191 (4th Cir.)

JOINT APPENDIX
Table of Contents

VOLUME 1

Exhibits to Wikimedia Foundation's Motion to Compel

Exhibits to Defendants' Opposition to Wikimedia Foundation's Motion to Compel

Exhibits to Wikimedia Foundation's Reply in Support of Its Motion to Compel

Opinion & Order Denying Wikimedia Foundation's Motion to Compel

Exhibits to Defendants' Motion for Summary Judgment

VOLUME 2

Exhibits to Wikimedia Foundation's Opposition to Defendants' Motion for Summary Judgment

VOLUME 3

Exhibits to Wikimedia Foundation's Opposition to Defendants' Motion for Summary Judgment (Cont'd)

VOLUME 4

Exhibits to Wikimedia Foundation's Opposition to Defendants' Motion for Summary Judgment (Cont'd)

VOLUME 5

Exhibits to Wikimedia Foundation's Opposition to Defendants' Motion for Summary Judgment (Cont'd)

VOLUME 6

Exhibits to Defendants' Reply in Support of Their Motion for Summary Judgment

VOLUME 7

Exhibits to Wikimedia Foundation's Sur-reply in Opposition to Defendants' Motion for Summary Judgment

Exhibits to Defendants' Sur-reply in Support of Their Motion for Summary Judgment

Opinion & Order Granting Defendants' Motion for Summary Judgment

Wikimedia Foundation's Notice of Appeal

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix AA

IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, INC. Plaintiff, v. NATIONAL SECURITY AGENCY, et al., Defendants.	Civil Action No. 1:15-cv-00662-TSE Hon. T.S. Ellis, III

WIKIMEDIA FOUNDATION, INC.'S SECOND AMENDED AND SUPPLEMENTAL RESPONSES AND OBJECTIONS TO NATIONAL SECURITY AGENCY'S FIRST SET OF INTERROGATORIES

PROPOUNDING PARTY: **NATIONAL SECURITY AGENCY**

RESPONDING PARTY: **WIKIMEDIA FOUNDATION, INC.**

SET NUMBER: **ONE**

Pursuant to Federal Rule of Civil Procedure 33, Plaintiff Wikimedia Foundation, Inc. ("Plaintiff" or "Wikimedia") amends and supplements its responses as follows to Defendant National Security Agency's ("Defendant" or "NSA") (collectively with Plaintiff, the "Parties") First Set of Interrogatories (the "Interrogatories"):

I. GENERAL RESPONSES.

1. Plaintiff's response to Defendant's Interrogatories is made to the best of Plaintiff's present knowledge, information, and belief. Discovery in this action is ongoing, and Plaintiff's responses may be substantially altered by further investigation, including further review of Plaintiff's own documents, as well as the review of documents produced by Defendant. Said response is at all times subject to such additional or different information that discovery or

further investigation may disclose and, while based on the present state of Plaintiff's recollection, is subject to such refreshing of recollection, and such additional knowledge of facts, as may result from Plaintiff's further discovery or investigation.

2. Plaintiff reserves the right to make any use of, or to introduce at any hearing and at trial, information and/or documents responsive to Defendant's Interrogatories but discovered subsequent to the date of this response, including, but not limited to, any such information or documents obtained in discovery herein.

3. To the extent that Plaintiff responds to Defendant's Interrogatories by stating that Plaintiff will provide information and/or documents that Plaintiff deems to embody material that is private, business confidential, proprietary, trade secret, or otherwise protected from disclosure pursuant to Federal Rule of Civil Procedure 26(c)(7), Federal Rule of Evidence 501, or other applicable law, Plaintiff will do so only pursuant to the Parties' Stipulated Protective Order (ECF No. 120).

4. Plaintiff reserves all objections or other questions as to the competency, relevance, materiality, privilege, or admissibility as evidence in any subsequent proceeding in or trial of this or any other action for any purpose whatsoever of Plaintiff's responses herein and any document or thing identified or provided in response to Defendant's Interrogatories.

5. Plaintiff's responses will be subject to and limited by any agreements the Parties reach concerning the scope of discovery.

6. Plaintiff reserves the right to object on any ground at any time to such other or supplemental interrogatories as Defendant may at any time propound involving or relating to the subject matter of these Interrogatories.

II. GENERAL OBJECTIONS.

Plaintiff makes the following general objections, whether or not separately set forth in response to each Interrogatory, to each instruction, definition, and Interrogatory made in Defendant's Interrogatories:

1. Plaintiff objects to the Interrogatories in their entirety insofar as any such instruction, definition, or Interrogatory seeks information or production of documents protected by the attorney-client privilege or the work product doctrine. Fed. R. Civ. Proc. 26(b)(1). Such information or documents shall not be provided in response to Defendant's Interrogatories and any inadvertent disclosure or production thereof shall not be deemed a waiver of any privilege with respect to such information or documents or of any work product immunity which may attach thereto. Fed. R. Civ. Proc. 26(b)(5)(B).

2. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory seeks identification of documents, witnesses, or information that Defendant has withheld from Plaintiff. Fed. R. Civ. Proc. 26(b)(1), (2).

3. Plaintiff objects to the Interrogatories in their entirety to the extent any such Interrogatory requires Plaintiff to identify potentially thousands of pages of documents, not all of which have been or can be located and reviewed by counsel within the time period allowed for this response or within a reasonable time. Accordingly, said Interrogatories would subject Plaintiff to unreasonable and undue annoyance, oppression, burden and expense.

4. Plaintiff objects to any Interrogatories that exceed the scope of jurisdictional discovery as defined by Defendants, *see* ECF No. 116 at 4, and ordered by the Court.

5. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory seeks information that is available through or from public

sources or records, or that are otherwise equally available to Defendant, on the ground that such instructions, definitions, and/or Interrogatories unreasonably subject Plaintiff to undue annoyance, oppression, burden, and expense. Fed. R. Civ. Proc. 26(b)(1), (2).

6. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory purport to impose obligations that are greater or more burdensome than or contradict those imposed by the applicable Federal and local rules. *See* Fed. R. Civ. Proc. 26, 33.

7. Plaintiff objects to the Interrogatories in their entirety as the Interrogatories contain more than the "25 written interrogatories, including all discrete subparts," permitted by the Federal Rules of Civil Procedure, Rule 33(a)(1), and Defendant has not sought leave to serve additional interrogatories.

8. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory seeks documents or information no longer in existence or not currently in Plaintiff's possession, custody, or control, or to the extent they refer to persons, entities, or events not known to Plaintiff or controlled by Plaintiff, on the grounds that such definitions or Interrogatories are overly broad, seek to require more of Plaintiff than any obligation imposed by law, would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense, and would seek to impose upon Plaintiff an obligation to investigate, discover, or produce information or materials from third parties or otherwise that are accessible to Defendant or readily obtainable from public or other sources. Fed. R. Civ. Proc. 26(b)(1), (2).

9. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory seeks information or production of documents protected

from disclosure by any right to privacy or any other applicable privilege or protection, including the right to confidentiality or privacy of third parties, any right of confidentiality provided for by Plaintiff's contracts or agreements with such third parties, or by Plaintiff's obligations under applicable law or contract to protect such confidential information. Plaintiff reserves the right to withhold any responsive information or documents governed by a third-party confidentiality agreement until such time as the appropriate notice can be given or the appropriate permissions can be obtained. Plaintiff also objects generally to all instructions, definitions, or Interrogatories to the extent they seek disclosure of trade secrets and other confidential research or analyses, development, or commercial information of Plaintiff or any third party.

10. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory is overbroad and unduly burdensome, particularly to the extent they seek "all," "each," or "any" documents, witnesses or facts relating to various subject matters. Fed. R. Civ. Proc. 26(b)(1), (2). To the extent Plaintiff responds to such Interrogatories, Plaintiff will use reasonable diligence to identify responsive documents, witnesses or facts in its possession, custody, or control, based on its present knowledge, information, and belief.

11. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory seeks expert discovery prematurely.

12. Plaintiff objects to any contention Interrogatories in their entirety as premature. Plaintiff will provide its response prior to the close of fact discovery.

13. Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory purports to require Plaintiff to restore and/or search data sources that are not reasonably accessible on the grounds that such definitions and Interrogatories would subject Plaintiff to undue burden and expense. Fed. R. Civ. Proc. 26(b)(1), (2).

III. DEFINITIONAL OBJECTIONS.

1. Plaintiff objects to definition number one (1) to the extent it defines "Plaintiff" and "Wikimedia" to include Plaintiff's "parent, subsidiary, and affiliated organizations, and all persons acting on their behalf, including officials, agents, employees, attorneys, and consultants." Said definition is overly broad, seeks irrelevant information not calculated to lead to the discovery of admissible evidence, seeks information outside of Plaintiff's possession, custody, or control, and would subject Plaintiff to unreasonable and undue annoyance, oppression, burden and expense. Said definition is also vague and ambiguous in that it cannot be determined what is meant by the terms "affiliated organizations" and "all persons acting on their behalf." Plaintiff shall construe "Plaintiff" and "Wikimedia" to mean Wikimedia, and its present officers, directors, agents, and employees.

2. Plaintiff objects to definition number four (4) and to each Interrogatory that purports to require Plaintiff to "state the basis of," "stating the basis of," "state on what basis," or otherwise "state with particularity" or "identify" "all" facts, documents, or persons whose testimony support or dispute any given factual assertion, on the ground that any response thereto would require subjective judgment on the part of Plaintiff and its attorneys, and would further require disclosure of a conclusion or opinion of counsel in violation of the attorney work product doctrine and/or attorney-client privilege. Plaintiff further objects that this definition and all requests to identify documents in the Interrogatories are premature at this early stage of the litigation, would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense, and would impose an obligation to provide information greater than that required by the Federal Rules of Civil Procedure.

3. Plaintiff objects to definition number five (5) as unduly burdensome in that it

purports to require Plaintiff to "identify" each "natural person" by providing information including "her most current home and business addresses, telephone numbers, and e-mail addresses, the name of her current employer, and her title."

4. Plaintiff objects to definition number six (6) as unduly burdensome in that it purports to require Plaintiff to "identify" an "entity that is not a natural person" by providing information including "its telephone number and e-mail address, and the full names, business addresses, telephone numbers, and e-mail addresses of both its chief executive officer and an agent designated by it to receive service of process."

5. Plaintiff objects to definition number seven (7) as unduly burdensome in that it purports to require Plaintiff to "identify" documents by providing "(a) the nature of the document (*i.e*, letter, memorandum, spreadsheet, database, etc.); (b) its date; (c) its author(s) (including title(s) or position(s)); (d) its recipient(s) (including title(s) or position(s)); (e) its number of pages or size; and (f) its subject matter," or by providing information in accordance with Defendant's "Specifications for Production of ESI and Digitized ('Scanned') Images attached to Defendant National Security Agency's First Set of Requests for Production." Plaintiff further objects that this definition and all requests to identify documents in the Interrogatories are premature at this early stage of the litigation, would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense, and would impose an obligation to provide information greater than that required by the Federal Rules of Civil Procedure.

IV. INSTRUCTIONAL OBJECTIONS

1. Plaintiff objects to instruction number one (1) to the extent it purports to request "knowledge or information" from Wikimedia's "parent, subsidiary, or affiliated organizations, and their officials, agents, employees, attorneys, consultants, and any other person acting on their

behalf." Said request is overly broad, seeks irrelevant information not calculated to lead to the discovery of admissible evidence, seeks information outside Plaintiff's possession, custody, or control, and would subject Plaintiff to unreasonable and undue annoyance, oppression, burden and expense. Moreover, said request is vague and ambiguous in that it cannot be determined what is meant by the term "affiliated organizations" and "any other person acting on their behalf." Where an Interrogatory requests knowledge or information of Plaintiff, Plaintiff shall construe such request to mean knowledge or information from Wikimedia, and its present officers, directors, agents, and employees.

2. Plaintiff objects to instruction number three (3) as unduly burdensome and imposing an obligation to provide information greater than that required by the Federal Rules of Civil Procedure to the extent it purports to require Plaintiff to "identify each person known by Plaintiff to have such knowledge, and in each instance where Plaintiff avers insufficient knowledge or information as a grounds for not providing information or for providing only a portion of the information requested, set forth a description of the efforts made to locate information needed to answer the interrogatory."

3. Plaintiff objects to instruction number four (4) to the extent it seeks to require it to identify anything other than the specific claim of privilege or work product being made and the basis for such claim, and to the extent it seeks to require any information not specified in Discovery Guideline 10, on the grounds that the additional information sought by Defendant would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense, and constitutes information protected from discovery by privilege and as work product. Plaintiff is willing to discuss acceptable reciprocal obligations for disclosure of information withheld on the basis of attorney-client privilege or attorney work-product.

4. Plaintiff objects to instruction number five (5) to the extent it defines "the time period for which each interrogatory seeks a response" as "the period from July 10, 2008 (the date of enactment of the FISA Amendments Act of 2008, Pub. L. 110-261, 121 Stat. 522) until the date of Plaintiff's response." This definition is overly broad, seeks irrelevant information not calculated to lead to the discovery of admissible evidence, and would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense. Where appropriate, Plaintiff has defined the specific time period encompassed by specific responses.

5. Plaintiff objects to instruction number six (6) that the Interrogatories are continuing, to the extent said instruction seeks unilaterally to impose an obligation to provide supplemental information greater than that required by Federal Rule of Civil Procedure 26(e) and would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense. Plaintiff will comply with the requirements of the Federal Rules of Civil Procedure and is willing to discuss mutually acceptable reciprocal obligations for continuing discovery.

V. SPECIFIC OBJECTIONS AND RESPONSES TO INTERROGATORIES.

Without waiving or limiting in any manner any of the foregoing General Objections, Definitional Objections, or Instructional Objections, but rather incorporating them into each of the following responses to the extent applicable, Plaintiff responds to the specific Interrogatories in Defendant's Interrogatories as follows:

INTERROGATORY NO. 2:

Unless Plaintiff's response to Interrogatory No. 1, above, is an unequivocal "no," then please state the basis of Plaintiff's contention that NSA Upstream surveillance involves the interception, copying, and review of all or substantially all international Internet text-based communications, including, but not limited to, the contentions that "Upstream surveillance is

intended to enable the comprehensive monitoring of international internet traffic," see Amended Complaint ¶ 48; that "the NSA is temporarily copying and then sifting through the contents of what is apparently most e mails and other text-based communications that cross the border," see id. ¶ 69; that "it would be difficult to systematically search the contents of the communications without first gathering nearly all cross-border text-based data," see Pl.'s Opp. to Defs.' MTD at 18-19; and that the U.S. Government "has acknowledged … that the NSA … examines the full contents of essentially everyone's communications to determine whether they include references to the NSA's search terms," *see id.* at 10.

RESPONSE TO INTERROGATORY NO. 2:

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory is a contention Interrogatory that is premature at this stage in the litigation. Plaintiff further submits that these matters may be the subject of expert testimony, as to which Plaintiff will provide discovery at the appropriate time.

Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery. Plaintiff additionally objects that this Interrogatory is improperly compound in that it contains multiple subparts.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

The bases for Plaintiff's contention include the following:

- Basic principles underlying how Internet communications are transmitted and how surveillance on a packet-switched network operates.

- Privacy & Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of FISA* (2014) ("PCLOB Report"), including pages 7–10, 12–

13, 22, 30–41 & n.157, 79, 111 n.476, 120–22, 125, 143, and official government sources concerning Upstream surveillance cited therein.

- [*Redacted*], No. [Redacted], 2011 WL 10945618 (FISC Oct. 3, 2011)
- 50 U.S.C. §§ 1801, 1881a.
- David S. Kris & J. Douglas Wilson, *National Security Investigations and Prosecutions* § 17.5 (July 2015)
- Julia Angwin & Jeff Larson, *New Snowden Documents Reveal Secret Memos Expanding Spying*, ProPublica (June 4, 2015) (and associated documents)
- Julia Angwin et al., *AT&T Helped U.S. Spy on Internet on Vast Scale*, N.Y. Times, Aug. 15, 2015 (and associated documents)
- Julia Angwin et al., *NSA Spying Relies on AT&T's 'Extreme Willingness to Help'*, ProPublica, Aug. 15, 2015 (and associated documents)
- Jeff Larson et al., *A Trail of Evidence Leading to AT&T's Partnership with the NSA*, ProPublica, Aug. 15, 2015 (and associated documents)
- PCLOB, Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 26:15–18 (Mar. 19, 2014) (statement of Robert Litt, General Counsel, ODNI)
- Charlie Savage, *Power Wars* (2015)

Additionally, Plaintiff's contention is based on the principles of Internet communication and the technical necessities of the inspection of Internet communications in transit.

For example, Internet communications in transit are split into packets. Where an eavesdropper is attempting to determine whether the contents of a particular communication in transit on the Internet contain a particular piece of information, the eavesdropper generally must

reassemble the packets constituting the communication and then scan the reassembled communication. Reassembling Internet packets requires the temporary copying (or "caching") of those packets until all packets needed for the reassembly have arrived.

Additionally, Upstream surveillance involves the retention of communications that contain targeted selectors. To retain a communication in transit, an eavesdropper must copy and reassemble the packets constituting the communication. But because an eavesdropper cannot know in advance which packets in transit are part of a communication containing a targeted selector, the eavesdropper must create a temporary copy of all packets that might be a part of such a communication.

The fact that all or substantially all international Internet text-based communications are subject to Upstream surveillance follows necessarily from the information the government has officially disclosed, and it is corroborated by independent news reports. For Upstream surveillance to serve the purposes the government has said it serves, the NSA must be comprehensively monitoring text-based communications originating or terminating in the United States. This is the only way for the NSA to reliably obtain communications to, from, and about its thousands of targets around the world, because those communications travel along paths in and out of the country that are unpredictable and change over time. Moreover, the structure of the Internet backbone facilitates such comprehensive surveillance. Because international communications are channeled through a small number of Internet chokepoints—and because the NSA's own documents show that it is conducting Upstream surveillance at many of those chokepoints—it is straightforward for the government to conduct the comprehensive surveillance necessary for Upstream to function as described.

The government's descriptions of Upstream surveillance make clear that the government

is interested in obtaining, with a high degree of confidence, all international communications to, from, and about its targets. For example, the Privacy and Civil Liberties Oversight Board has described the use of Upstream surveillance to collect "about" communications as "an inevitable byproduct of the government's efforts to *comprehensively* acquire communications that are sent to or from its targets." PCLOB Report 10 (emphasis added). And it has said about Upstream surveillance more generally that this method's "success . . . depends on collection devices that can reliably acquire data packets associated with the proper communications." *Id.* at 143 (emphasis added).

Because the routing of Internet traffic is unpredictable, however, the government can only "comprehensively" and "reliably" obtain communications to, from, and about its thousands of targets by conducting its surveillance on the different routes by which Internet communications enter and leave the country, and by examining substantially all international communications that travel those various routes.

The path that an Internet communication takes is inherently unpredictable. Internet communications are routed around the globe based on a complex set of rules and relationships that are applied dynamically, based on network conditions at any given moment. These network conditions change frequently, and so one cannot know in advance which path a particular communication will travel. Indeed, even the communications between two individuals in a single conversation (such as an Internet chat or email exchange) may take entirely different routes across the Internet backbone, even though the end-points are the same. For example, if an NSA target is having an Internet chat conversation with someone in the United States, the communications *from* the target will frequently follow a different path than those *to* the target. And, of course, a target's location may vary over time. For all these reasons, a target's

communications may traverse one Internet circuit at one moment, but a different one later.

The fact that the NSA had, at last public count, 106,469 surveillance targets (some of which are groups with perhaps hundreds or even thousands of members) only reinforces the conclusion that Upstream surveillance of international text-based communications must be comprehensive. *See* ODNI, Statistical Transparency Report Regarding the Use of National Security Authorities for Calendar Year 2016 (Apr. 2017), https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2016. The communications of so many targets scattered around the world will travel many different routes across the Internet backbone, based on the locations of those various targets, their individual movements over time, and changes in network conditions. These communications will be intermingled with those of the general population in the flow of Internet traffic. An intelligence agency that seeks to reliably intercept communications to, from, or about its targets, could do so only by searching substantially all text-based communications entering or leaving the country.

This allegation is based on the government's official disclosures and on necessary inferences from those disclosures, but it is also corroborated by news accounts. A *New York Times* report from August 2013 states, based on a review of NSA documents and interviews with senior intelligence officials, that "the N.S.A. is temporarily copying and then sifting through the contents of what is apparently most e-mails and other text-based communications that cross the border." Charlie Savage, *N.S.A. Said to Search Content of Messages to and from U.S.*, N.Y. Times, Aug. 8, 2013, http://nyti.ms/1E1nlsi. The same *New York Times* report also explains why the NSA's Upstream surveillance is so far-reaching:

> "Computer scientists said that it would be difficult to systematically search the contents of the communications without first gathering nearly all cross-border text-based data;

> fiber-optic networks work by breaking messages into tiny packets that flow at the speed of light over different pathways to their shared destination, so they would need to be captured and reassembled."

Id.; see also Charlie Savage, *Power Wars* 207–11 (2015).

Not only does the NSA have an overriding incentive to copy and review substantially all international Internet communications, but the Internet backbone is structured in a way that enables it to do so.

The Internet backbone funnels almost all Internet communications entering and leaving the country through a limited number of chokepoints. The Internet backbone includes a relatively small number of international submarine cables (and a limited number of terrestrial cables) that transport Internet traffic into and out of the United States. Because there are relatively few high-capacity cables carrying international Internet communications, there are correspondingly few chokepoints—*i.e.*, junctions through which all international Internet communications must pass en route to their destinations. By installing its surveillance equipment at the small number of backbone chokepoints, the NSA is able to monitor substantially all text-based communications entering or leaving the United States. And the government has acknowledged that it conducts Upstream surveillance at international links and on the Internet backbone. [*Redacted*], 2011 WL 10945618, at *15; PCLOB Report 36–37.

NSA documents published in the press show that the NSA has installed surveillance equipment at many major chokepoints on the Internet backbone. One of these NSA documents states that the NSA has established interception capabilities on "many of the chokepoints operated by U.S. providers through which international communications enter and leave the United States." *See* Plaintiff's First Amended Complaint ¶ 69. Another shows that just one of

those participating providers has facilitated Upstream surveillance at seven major international chokepoints in the United States. *Id.* ¶ 68. Additional reporting states that the NSA has installed surveillance equipment in at least 17 "internet hubs" operated by another major U.S. telecommunications provider. Julia Angwin et al., *NSA Spying Relies on AT&T's 'Extreme Willingness to Help'*, ProPublica, Aug. 15, 2015 (and associated documents).

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 2:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement as discovery in this case continues, Plaintiff supplements its response as follows:

The bases for Plaintiff's contention also include the following: Glenn Greenwald, *No Place to Hide* (2014).

The fact that the NSA had, at last public count, 106,469 surveillance targets (some of which are groups with perhaps hundreds or even thousands of members) only reinforces the conclusion that Upstream surveillance of international text-based communications must be comprehensive. *See* ODNI, Statistical Transparency Report Regarding the Use of National Security Authorities for Calendar Year 2016 (Apr. 2017), https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2016; *see generally* ODNI Statistical Transparency Reports Regarding the Use of National Security Authorities.

SECOND SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 2:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement as discovery in this case continues, Plaintiff supplements its response as follows:

The bases for Plaintiff's contention also include the following:

- PCLOB, Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (Mar. 19, 2014)
- PCLOB, Public Hearing Regarding Consideration of Recommendations for Change: The Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act (Nov. 4, 2013)
- June 1, 2011 FISC submission
- July 15, 2015 FISC submission (2015 Summary of Notable Section 702 Requirements)
- June 28, 2011 FISC submission
- August 16, 2011 FISC submission
- November 15, 2011 FISC submission (Government's Responses to FISC Questions Re: Amended 2011 Section 702 Certifications)
- FISC Opinion (Sept. 25, 2012)
- FISC Opinion (Apr. 26, 2017)
- NSA Section 702 Targeting Procedures
- NSA Section 702 Minimization Procedures
- PCLOB, Recommendations Assessment Reports
- Executive Office of the President of the United States, The Comprehensive National Cybersecurity Initiative
- U.S. Dep't of Homeland Security, Privacy Impact Assessment for the Initiative Three Exercise (Mar. 18, 2010)

- OLC, Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection System (Einstein 2.0) to Protect Unclassified Computer Networks in the Executive Branch (Jan. 9, 2009)
- U.S. Dep't of Homeland Security, Privacy Impact Assessment for Einstein 3 – Accelerated (E3A) (Apr. 19, 2013)
- U.S. Dep't of Homeland Security, Privacy Impact Assessment for Einstein 2 (May 19, 2008)

INTERROGATORY NO. 6:

For each category of Wikimedia international, text-based, Internet communications identified in response to Interrogatory No. 3, above, that Plaintiff contends is intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance, please identify each foreign country to or from which such Wikimedia communications were sent in the past 24 months.

RESPONSE TO INTERROGATORY NO. 6:

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory is overbroad, unduly burdensome and seeks information that is not reasonably calculated to lead to the discovery of admissible evidence. Plaintiff also objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff further objects that this Interrogatory seeks information that exceeds the scope of jurisdictional discovery as defined by Defendants, see ECF No. 116 at 4, and as ordered by the Court.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

(1) Wikimedia communications with its community members. Between April 23,

2017 and December 31, 2017, Wikimedia's U.S. servers received HTTPS requests from, and transmitted HTTPS responses to, users in at least 242 non-U.S. countries, territories and regions. This figure is an estimate that was derived using MaxMind geolocation data to determine the country associated with the client IP of each HTTPS request transmitted to Wikimedia's servers in the United States.

(2) Wikimedia's internal log communications. Every time Wikimedia receives an HTTPS request from a person accessing a Wikimedia Project webpage, it creates a corresponding log entry. Between April 23, 2017 and December 31, 2017, Wikimedia's servers in Amsterdam transmitted over 970 billion logs to Wikimedia's servers in the United States.

(3) Electronic communications of Wikimedia staff. Between January 1, 2015 and December 12, 2017, Wikimedia's office network router located in the United States sent Internet communications to at least approximately 221 non-U.S. countries, territories and regions.

This figure represents Internet outbound communications sent via the following Internet protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

This figure includes communications sent through Wikimedia's Virtual Private Network (VPN).

This figure does not account for the significant number of Internet communications by Wikimedia staff and contractors located internationally, who did not communicate using Wikimedia's Virtual Private Network, but who routinely communicate with Wikimedia staff located at the U.S. headquarters. Between January 1, 2015 and December 22, 2017, Wikimedia engaged over 80 contractors, located across more than 30 different countries.

The results of these analyses will be produced to Defendants. An anonymized list of

Plaintiff's contractors located abroad will also be produced to Defendants.

AMENDED RESPONSE TO INTERROGATORY NO. 6:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement or amend its response as discovery in this case continues, Plaintiff amends its response as follows:

(1) Wikimedia communications with its community members. Between April 23, 2017 and December 31, 2017, Wikimedia's U.S. servers received HTTP/S requests from, and transmitted HTTP/S responses to, users in at least 242 non-U.S. countries, territories and regions. This figure is an estimate that was derived using MaxMind geolocation data to determine the country associated with the client IP of each HTTPS request transmitted to Wikimedia's servers in the United States.

(2) Wikimedia's internal log communications. Every time Wikimedia receives an HTTP/S request from a person accessing a Wikimedia Project webpage, it creates a corresponding log entry. Between April 23, 2017 and December 31, 2017, Wikimedia's servers in Amsterdam transmitted approximately over 970 billion logs to Wikimedia's servers in the United States.

(3) Electronic communications of Wikimedia staff. Between January 1, 2015 and December 12, 2017, Wikimedia's office network router located in the United States logged open Internet connections with at least approximately 221 non-U.S. countries, territories and regions.

This figure represents Internet outbound communications sent via the following Internet protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

This figure includes, but is not limited to, certain communications sent through

Wikimedia's Virtual Private Network (VPN).

This figure does not account for a significant number of Internet communications by Wikimedia staff and contractors located internationally who routinely communicate with Wikimedia staff and others located in the United States without using Wikimedia's Virtual Private Network. Between January 1, 2015 and December 22, 2017, Wikimedia engaged over 140 contractors, located across approximately 45 different countries.

The results of these analyses have been produced to Defendants. *See* WIKI0006146, WIKI0006147, WIKI0006148, WIKI0006149, WIKI0006282, WIKI0006368. An anonymized list of Plaintiff's contractors located abroad has also been produced to Defendants. *See* WIKI0006367.

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 6:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement its response as discovery in this case continues, Plaintiff supplements its response as follows:

The results of additional analyses on these three categories of communications are contained in response to Defendant Office of the Director of National Intelligence's Interrogatory No. 19.

INTERROGATORY NO. 7:

For each category of Wikimedia international, text-based, Internet communications identified in response to Interrogatory No. 3, above, that Plaintiff contends is intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance, please state the total number of such Wikimedia communications made to and from the United States each year for the years 2008-2017, specifying in each case the manner in which Wikimedia counts the communications

in that category (e.g., by site visit, page view, HTTP or HTTPS transmissions, e-mails, other forms of messaging, etc.).

RESPONSE TO INTERROGATORY NO. 7:

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory is vastly overbroad, unduly burdensome and seeks information that is not reasonably calculated to lead to the discovery of admissible evidence. Plaintiff also objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff further objects that this Interrogatory seeks information that exceeds the scope of jurisdictional discovery as defined by Defendants, see ECF No. 116 at 4, and as ordered by the Court.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

(1) Wikimedia communications with its community members. Between April 23, 2017 and December 31, 2017, Wikimedia's U.S. servers received over 500 billion HTTPS requests from users outside of the United States. Each HTTPS request generates a corresponding response; thus Wikimedia exchanged over 1 trillion HTTPS requests and responses with its users between April 23, 2017 and December 31, 2017. These figures are estimates that were derived using MaxMind geolocation data to determine the country associated with the client IP of each HTTPS request transmitted to Wikimedia's servers in the United States.

(2) Wikimedia's internal log communications. Between April 23, 2017 and December 31, 2017, Wikimedia's servers in Amsterdam transmitted approximately over 970 billion logs to Wikimedia's servers in the United States.

(3) Electronic communications of Wikimedia staff. Between June 4, 2014 and

December 12, 2017, Wikimedia's office network router located in the United States made at least approximately 22,934,372 Internet connections to 223 non-U.S. countries, territories and regions.

This figure is an estimate and was derived using a geolocation database that catalogues the IP addresses associated with each country, territory and region for each log entry obtained from the Wikimedia Foundation's office router.

This figure represents the total number of Internet outbound connections sent via the following Internet protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

This figure includes connections sent through Wikimedia's Virtual Private Network (VPN).

This figure does not account for the significant number of Internet communications by Wikimedia staff and contractors located internationally who did not communicate using Wikimedia's Virtual Private Network, but who routinely communicate with Wikimedia staff located at the U.S. headquarters. Between January 1, 2015 and December 22, 2017, Wikimedia engaged over 80 contractors, located across more than 30 different countries.

The results of these analyses will be produced to Defendants. An anonymized list of Plaintiff's contractors located abroad will also be produced to Defendants.

AMENDED RESPONSE TO INTERROGATORY NO. 7:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement or amend its response as discovery in this case continues, Plaintiff amends its response as follows:

(1) Wikimedia communications with its community members. Between April 23, 2017 and December 31, 2017, Wikimedia's U.S. servers received approximately over 511 billion

HTTP/S requests from users outside of the United States. Each HTTP/S request generates a corresponding response; thus Wikimedia exchanged over 1 trillion HTTP/S requests and responses with its users between April 23, 2017 and December 31, 2017.

These figures are estimates that were derived using MaxMind geolocation data to determine the country associated with the client IP of each HTTP/S request transmitted to Wikimedia's servers in the United States.

(2) Wikimedia's internal log communications. Between April 23, 2017 and December 31, 2017, Wikimedia's servers in Amsterdam transmitted approximately over 970 billion logs to Wikimedia's servers in the United States.

(3) Electronic communications of Wikimedia staff. Between June 4, 2014 and December 12, 2017, Wikimedia's office network router located in the United States logged open Internet connections at least approximately 22,934,372 times, with 223 non-U.S. countries, territories and regions.

This figure is an estimate and was derived using a geolocation database that catalogues the IP addresses associated with each country, territory and region for each log entry obtained from the Wikimedia Foundation's office router.

This figure represents the total number of Internet outbound connections sent via the following Internet protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

This figure includes, but is not limited to, connections sent through Wikimedia's Virtual Private Network (VPN).

This figure does not account for a significant number of Internet communications by Wikimedia staff and contractors located internationally who routinely communicate with

Wikimedia staff and others located in the United States without using Wikimedia's Virtual Private Network. Between January 1, 2015 and December 22, 2017, Wikimedia engaged over 140 contractors, located across approximately 45 different countries.

The results of these analyses have been produced to Defendants. *See* WIKI0006146, WIKI0006147, WIKI0006148, WIKI0006149, WIKI0006282, WIKI0006368. An anonymized list of Plaintiff's contractors located abroad has also been produced to Defendants. *See* WIKI0006367.

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 7:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement its response as discovery in this case continues, Plaintiff supplements its response as follows:

The results of additional analyses on these three categories of communications are contained in response to Defendant Office of the Director of National Intelligence's Interrogatory No. 19.

INTERROGATORY NO. 8:

For each category of Wikimedia international, text-based, Internet communications identified in response to Interrogatory No. 3, above, that Plaintiff contends is intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance, please state by foreign country the number of such Wikimedia communications made to or from the United States each year for the years 2008-2017, specifying in each case the manner in which Wikimedia counts the communications in that category (e.g., by site visit, page view, HTTP or HTTPS transmissions, e-mails, other forms of messaging, etc.).

RESPONSE TO INTERROGATORY NO. 8:

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory is vastly overbroad, unduly burdensome and seeks information that is not reasonably calculated to lead to the discovery of admissible evidence. Plaintiff also objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff further objects that this Interrogatory seeks information that exceeds the scope of jurisdictional discovery as defined by Defendants, *see* ECF No. 116 at 4, and as ordered by the Court. Plaintiff additionally objects to this Interrogatory as duplicative of other written discovery propounded by Defendants.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

(1) Wikimedia communications with its community members. The number of HTTPS requests that Wikimedia's U.S. servers received from users in each country, territory, or region between April 23, 2017 and December 31, 2017 is attached as Exhibit B and will be included in a forthcoming production to Defendants. Each HTTPS request generates a corresponding response that is not reflected in the figures included in this analysis. These figures are estimates that were derived using MaxMind geolocation data to determine the country associated with the client IP of each HTTPS request transmitted to Wikimedia's servers in the United States.

(2) Wikimedia's internal log communications. Between April 23, 2017 and December 31, 2017, Wikimedia's servers in Amsterdam transmitted over 970 billion logs to Wikimedia's servers in the United States.

(3) Electronic communications of Wikimedia staff. Between June 4, 2014 and

December 12, 2017, Wikimedia's office network router located in the United States sent at least approximately 22,934,372 Internet connections to at least 223 non-U.S. countries, territories and regions. A list of the numbers of these communications broken down by country, territory, or region will be produced to Defendants.

These figures are estimates and were derived using a geolocation database that catalogues the IP addresses associated with each country, territory and region for each log entry obtained from the Wikimedia Foundation's office router.

These figures represent the total number of Internet outbound connections sent via the following Internet protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

These figures include connections sent through Wikimedia's Virtual Private Network (VPN).

These figures do not account for the significant number of Internet communications by Wikimedia staff and contractors located internationally who did not communicate using Wikimedia's Virtual Private Network, but who routinely communicate with Wikimedia staff located at the U.S. headquarters. Between January 1, 2015 and December 22, 2017, Wikimedia engaged over 80 contractors, located across more than 30 different countries.

The results of these analyses will be produced to Defendants. An anonymized list of Plaintiff's staff and contractors located abroad will also be produced to Defendants.

AMENDED RESPONSE TO INTERROGATORY NO. 8:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement or amend its response as discovery in this case continues, Plaintiff amends its response as follows:

(1) Wikimedia communications with its community members. The number of HTTP/S requests that Wikimedia's U.S. servers received from users in each country, territory, or region between April 23, 2017 and December 31, 2017 is attached as Amended Exhibit B. Each HTTP/S request generates a corresponding response that is not reflected in the figures included in this analysis. These figures are estimates that were derived using MaxMind geolocation data to determine the country associated with the client IP of each HTTP/S request transmitted to Wikimedia's servers in the United States.

(2) Wikimedia's internal log communications. Between April 23, 2017 and December 31, 2017, Wikimedia's servers in Amsterdam transmitted approximately over 970 billion logs to Wikimedia's servers in the United States.

(3) Electronic communications of Wikimedia staff. Between June 4, 2014 and December 12, 2017, Wikimedia's office network router located in the United States logged open Internet connections at least approximately 22,934,372 times with 223 non-U.S. countries, territories and regions. A list of the numbers of these communications broken down by country, territory, or region will be produced to Defendants.

This figure is an estimate and was derived using a geolocation database that catalogues the IP addresses associated with each country, territory and region for each log entry obtained from the Wikimedia Foundation's office router.

This figure represents the total number of Internet outbound connections sent via the following Internet protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

This figure includes, but is not limited to, connections sent through Wikimedia's Virtual Private Network (VPN).

This figure does not account for a significant number of Internet communications by Wikimedia staff and contractors located internationally who routinely communicate with Wikimedia staff and others located in the United States without using Wikimedia's Virtual Private Network. Between January 1, 2015 and December 22, 2017, Wikimedia engaged over 140 contractors, located across approximately 45 different countries.

The results of these analyses have been produced to Defendants. *See* WIKI0006146, WIKI0006147, WIKI0006148, WIKI0006149, WIKI0006282, WIKI0006368. An anonymized list of Plaintiff's staff and contractors located abroad has also been produced to Defendants. *See* WIKI0006367.

SECOND AMENDED RESPONSE TO INTERROGATORY NO. 8:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement or amend its response as discovery in this case continues, Plaintiff amends its response as follows:

(1) Wikimedia communications with its community members. The number of HTTP/S requests that Wikimedia's U.S. servers received from users in each country, territory, or region between April 23, 2017 and December 31, 2017 is attached as Amended Exhibit B. The number of HTTP requests that Wikimedia's U.S. servers received from users in each country, territory, or region between August 1, 2017 and January 31, 2018 is attached as Supplemental Exhibit C. The number of HTTPS requests that Wikimedia's U.S. servers received from users in each country territory, or region between August 1, 2017 and January 31, 2018 is attached as Supplemental Exhibit D. Each HTTP/S request generates a corresponding response that is not reflected in the figures included in this analysis. These figures are estimates that were derived using MaxMind geolocation data to determine the country associated with the client IP of each

HTTP/S request transmitted to Wikimedia's servers in the United States.

(2) Wikimedia's internal log communications. Between April 23, 2017 and December 31, 2017, Wikimedia's servers in Amsterdam transmitted approximately over 970 billion logs to Wikimedia's servers in the United States.

(3) Electronic communications of Wikimedia staff. Between June 4, 2014 and December 12, 2017, Wikimedia's office network router located in the United States logged open Internet connections at least approximately 22,934,372 times with 223 non-U.S. countries, territories and regions. A list of the numbers of these communications broken down by country, territory, or region will be produced to Defendants.

This figure is an estimate and was derived using a geolocation database that catalogues the IP addresses associated with each country, territory and region for each log entry obtained from the Wikimedia Foundation's office router.

This figure represents the total number of Internet outbound connections sent via the following Internet protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

This figure includes, but is not limited to, connections sent through Wikimedia's Virtual Private Network (VPN).

This figure does not account for a significant number of Internet communications by Wikimedia staff and contractors located internationally who routinely communicate with Wikimedia staff and others located in the United States without using Wikimedia's Virtual Private Network. Between January 1, 2015 and December 22, 2017, Wikimedia engaged over 140 contractors, located across approximately 45 different countries.

The results of these analyses have been produced to Defendants. *See* WIKI0006146,

WIKI0006147, WIKI0006148, WIKI0006149, WIKI0006282, WIKI0006368. An anonymized list of Plaintiff's staff and contractors located abroad has also been produced to Defendants. *See* WIKI0006367.

The results of additional analyses on these three categories of communications are contained in response to Defendant Office of the Director of National Intelligence's Interrogatory No. 19.

INTERROGATORY NO. 11:

Please state the basis of Plaintiff's allegations, in paragraphs 61, 85, and 88 of the Amended Complaint, that Wikimedia's alleged "community of volunteers, contributors, and readers consists of individuals in virtually every country on earth" and that Wikimedia "communicate[s] with individuals in virtually every country on earth."

RESPONSE TO INTERROGATORY NO. 11:

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is overbroad and duplicative of other written discovery propounded by Defendants. Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

Numerous facts support Wikimedia's allegations that its "community of volunteers, contributors, and readers consists of individuals in virtually every country on earth" and that Wikimedia engages in "communications . . . with individuals in virtually every country on earth." As explained in Wikimedia's responses to NSA Interrogatory Nos. 6-8, Wikimedia users from all over the world read and contribute to Wikimedia's Project pages. This analysis is further supported by statistics showing that Wikimedia's Project pages are viewed by millions of users around the world. Wikimedia publishes current monthly page view statistics by country

(*available* at https://stats.wikimedia.org/wikimedia/squids/SquidReportPageViewsPerCountryOverview.htm), and maintains an archive with analogous data for past months (*available* at https://stats.wikimedia.org/archive/squid_reports/).

Wikimedia also has dozens of foreign independent but associated entities, including user groups, chapters and thematic organizations. *See* https://meta.wikimedia.org/wiki/Wikimedia_movement_affiliates#chapters.

In the last two years alone, Wikimedia has awarded grants and scholarships to users and programs in dozens of countries. Additionally, Wikimedia projects are currently active in 288 languages, further underscoring Wikimedia's global presence. *See* https://en.wikipedia.org/wiki/List_of_Wikipedias.

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 11:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement its response as discovery in this case continues, Plaintiff supplements its response as follows:

Wikimedia also maintains a publicly available repository of data that allows for various analyses of Wikimedia project page views by country (*available* at https://wikitech.wikimedia.org/wiki/Analytics/AQS/Pageviews).

Numerous documents in Plaintiff's production support its allegations that its "community of volunteers, contributors, and readers consists of individuals in virtually every country on earth" and that Wikimedia engages in "communications . . . with individuals in virtually every country on earth," including, *inter alia*, Amended Exhibit B; WIKI0006367 (listing international Wikimedia contractors); WIKI0002407 (listing 288 Wikipedia language editions);

WIKI0002416 (listing Wikimedia movement affiliates); WIKI0006369 (listing page views for virtually every country on earth); WIKI0002360, WIKI0002365, WIKI0002367, WIKI0002389, WIKI0002396 (noting countries involved in user grants and scholarships); WIKI0006295 (listing funded grants by country).

SECOND SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 11:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement its response as discovery in this case continues, Plaintiff supplements its response as follows:

Numerous other statistics produced by Plaintiff show that Wikimedia's community of volunteers, contributors, and readers consists of individuals in virtually every country on earth, and that Wikimedia engages in communications with individuals in virtually every country on earth. *See* WIKI0009301, WIKI0008312, WIKI0008313, WIKI0007616, WIKI0009269, WIKI0008265, WIKI0008271, WIKI0008262, WIKI0009224, WIKI0009234.

ALLEGATIONS REGARDING NSA INTERCEPTION OF WIKIMEDIA'S INTERNATIONAL, TEXT-BASED, INTERNET COMMUNICATIONS

INTERROGATORY NO. 14:

Please state the basis of Plaintiff's allegation, in paragraph 49 of the Amended Complaint, that Upstream surveillance includes a process in which the NSA makes a copy of international text-based communications flowing across certain high-capacity cables, switches, and routers along the Internet backbone.

RESPONSE TO INTERROGATORY NO. 14:

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is duplicative of other written discovery propounded by Defendants.

Plaintiff additionally objects that these matters may be the subject of expert reports and

testimony, as to which Plaintiff will provide discovery at the appropriate time.

Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

The bases of Plaintiff's allegation are the principles of Internet communication and the technical necessities of the inspection of Internet communications in transit.

For example, Internet communications in transit are split into packets. Where an eavesdropper is attempting to determine whether the contents of a particular communication in transit on the Internet contain a particular piece of information, the eavesdropper generally must reassemble the packets constituting the communication and then scan the reassembled communication. Reassembling Internet packets requires the temporary copying (or "caching") of those packets until all packets needed for the reassembly have arrived.

Additionally, Upstream surveillance involves the retention of communications that contain targeted selectors. To retain a communication in transit, an eavesdropper must copy and reassemble the packets constituting the communication. But because an eavesdropper cannot know in advance which packets in transit are part of a communication containing a targeted selector, the eavesdropper must create a temporary copy of all packets that might be a part of such a communication.

In addition, a *New York Times* report from August 2013 states, based on a review of NSA documents and interviews with senior intelligence officials, that "the N.S.A. is temporarily copying and then sifting through the contents of what is apparently most e-mails and other textbased communications that cross the border." Charlie Savage, *N.S.A Said to Search Content*

of Messages to and from U.S., N.Y. Times, Aug. 8, 2013; *see also* Charlie Savage, *Power Wars* 207–11 (2015).

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 14:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement its response as discovery in this case continues, Plaintiff supplements its response as follows:

The bases for Plaintiff's allegation also include the following:

- Executive Office of the President of the United States, The Comprehensive National Cybersecurity Initiative
- U.S. Dep't of Homeland Security, Privacy Impact Assessment for the Initiative Three Exercise (Mar. 18, 2010)
- OLC, Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection System (Einstein 2.0) to Protect Unclassified Computer Networks in the Executive Branch (Jan. 9, 2009)
- U.S. Dep't of Homeland Security, Privacy Impact Assessment for Einstein 3 – Accelerated (E3A) (Apr. 19, 2013)
- U.S. Dep't of Homeland Security, Privacy Impact Assessment for Einstein 2 (May 19, 2008)

INTERROGATORY NO. 15:

Please state the basis of Plaintiff's contentions regarding the manner in which the alleged copying, filtering, and content-review processes referred to in paragraph 49 of the Amended Complaint are carried out.

RESPONSE TO INTERROGATORY NO. 15:

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is a contention Interrogatory that is premature at this stage in the litigation. Plaintiff additionally objects that these matters may be the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time.

Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery. Plaintiff also objects that this Interrogatory is overbroad and duplicative of other written discovery propounded by Defendants.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

The bases of Plaintiff's contentions are the principles of Internet communication and the technical necessities of the inspection of Internet communications in transit.

For example, Internet communications in transit are split into packets. Where an eavesdropper is attempting to determine whether the contents of a particular communication in transit on the Internet contain a particular piece of information, the eavesdropper generally must reassemble the packets constituting the communication and then scan the reassembled communication. Reassembling Internet packets requires the temporary copying (or "caching") of those packets until all packets needed for the reassembly have arrived.

Additionally, Upstream surveillance involves the retention of communications that contain targeted selectors. To retain a communication in transit, an eavesdropper must copy and reassemble the packets constituting the communication. But because an eavesdropper cannot know in advance which packets in transit are part of a communication containing a targeted selector, the eavesdropper must create a temporary copy of all packets that might be a part of

such a communication.

In addition, a *New York Times* report from August 2013 states, based on a review of NSA documents and interviews with senior intelligence officials, that "the N.S.A. is temporarily copying and then sifting through the contents of what is apparently most e-mails and other text-based communications that cross the border." Charlie Savage, *N.S.A Said to Search Content of Messages to and from U.S.*, N.Y. Times, Aug. 8, 2013; *see also* Charlie Savage, *Power Wars* 207–11 (2015).

Other bases of Plaintiff's contentions include:

- The PCLOB Report, including pages 7–10, 12–13, 22, 30–41 & n.157, 79, 111 n.476, 120–22, 125, 143, and official government sources concerning Upstream surveillance cited therein.
- [*Redacted*], No. [Redacted], 2011 WL 10945618 (FISC Oct. 3, 2011)
- 50 U.S.C. §§ 1801, 1881a.
- David S. Kris & J. Douglas Wilson, *National Security Investigations and Prosecutions* § 17.5 (July 2015)
- Julia Angwin et al., *NSA Spying Relies on AT&T's 'Extreme Willingness to Help'*, ProPublica, Aug. 15, 2015 (and associated documents)
- Julia Angwin & Jeff Larson, *New Snowden Documents Reveal Secret Memos Expanding Spying*, ProPublica, June 4, 2015 (and associated documents)
- Jeff Larson et al., *A Trail of Evidence Leading to AT&T's Partnership with the NSA*, ProPublica, Aug. 15, 2015 (and associated documents)
- PCLOB, Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 26:15–18 (Mar. 19, 2014) (statement of

Robert Litt, General Counsel, ODNI)

- Charlie Savage, *Power Wars* (2015)

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 15:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement as discovery in this case continues, Plaintiff supplements its response as follows:

The bases for Plaintiff's contention also include the following: Glenn Greenwald, *No Place to Hide* (2014).

SECOND SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 15:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement as discovery in this case continues, Plaintiff supplements its response as follows:

The bases for Plaintiff's contentions also include the following:

- PCLOB, Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (Mar. 19, 2014)
- PCLOB, Public Hearing Regarding Consideration of Recommendations for Change: The Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act (Nov. 4, 2013)
- June 1, 2011 FISC submission
- July 15, 2015 FISC submission (2015 Summary of Notable Section 702 Requirements)
- June 28, 2011 FISC submission
- August 16, 2011 FISC submission

- November 15, 2011 FISC submission (Government's Responses to FISC Questions Re: Amended 2011 Section 702 Certifications)
- FISC Opinion (Sept. 25, 2012)
- FISC Opinion (Apr. 26, 2017)
- NSA Section 702 Targeting Procedures
- NSA Section 702 Minimization Procedures
- PCLOB, Recommendations Assessment Reports
- ODNI, Statistical Transparency Reports Regarding the Use of National Security Authorities
- Executive Office of the President of the United States, The Comprehensive National Cybersecurity Initiative
- U.S. Dep't of Homeland Security, Privacy Impact Assessment for the Initiative Three Exercise (Mar. 18, 2010)
- OLC, Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection System (Einstein 2.0) to Protect Unclassified Computer Networks in the Executive Branch (Jan. 9, 2009)
- U.S. Dep't of Homeland Security, Privacy Impact Assessment for Einstein 3 – Accelerated (E3A) (Apr. 19, 2013)
- U.S. Dep't of Homeland Security, Privacy Impact Assessment for Einstein 2 (May 19, 2008)
- ODNI, Conference Call with the Press Addressing Multi-Communication Transactions (Aug. 21, 2013)

INTERROGATORY NO. 17:

Please state the basis of Plaintiff's allegations, in paragraphs 62 and 64 of the Amended Complaint, respectively, that "in order for the NSA to reliably obtain communications to, from, or about its targets in the way it has described, the government must be copying and reviewing all the international text-based communications that travel across a given link," and that "for every backbone link that the NSA monitors using Upstream surveillance, the monitoring must be comprehensive in order for the government to accomplish its stated goals."

RESPONSE TO INTERROGATORY NO. 17:

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff also objects that this Interrogatory is duplicative of other written discovery propounded by Defendants. Plaintiff additionally objects that these matters may be the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time. Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

Plaintiff's allegation is based on basic principles governing the routing and transmission of Internet communications, as well as basic principles governing how surveillance on a packet-switched network operates.

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 17:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement as discovery in this case continues, Plaintiff supplements its

response as follows:

The bases for Plaintiff's allegations also include the following:

- PCLOB Report and official government sources concerning Upstream surveillance cited therein.
- [*Redacted*], No. [Redacted], 2011 WL 10945618 (FISC Oct. 3, 2011)
- 50 U.S.C. §§ 1801, 1881a
- David S. Kris & J. Douglas Wilson, *National Security Investigations and Prosecutions* § 17.5 (July 2015)
- Julia Angwin & Jeff Larson, *New Snowden Documents Reveal Secret Memos Expanding Spying*, ProPublica (June 4, 2015) (and associated documents)
- Julia Angwin et al., *AT&T Helped U.S. Spy on Internet on Vast Scale*, N.Y. Times, Aug. 15, 2015 (and associated documents)
- Julia Angwin et al., *NSA Spying Relies on AT&T's 'Extreme Willingness to Help'*, ProPublica, Aug. 15, 2015 (and associated documents)
- Jeff Larson et al., *A Trail of Evidence Leading to AT&T's Partnership with the NSA*, ProPublica, Aug. 15, 2015 (and associated documents)
- Charlie Savage, *Power Wars* (2015)
- Charlie Savage, *N.S.A. Said to Search Content of Messages to and from U.S.*, N.Y. Times, Aug. 8, 2013
- Glenn Greenwald, *No Place to Hide* (2014)
- PCLOB, Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (Mar. 19, 2014)

- PCLOB, Public Hearing Regarding Consideration of Recommendations for Change: The Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act (Nov. 4, 2013)
- June 1, 2011 FISC submission
- July 15, 2015 FISC submission (2015 Summary of Notable Section 702 Requirements)
- June 28, 2011 FISC submission
- August 16, 2011 FISC submission
- November 15, 2011 FISC submission (Government's Responses to FISC Questions Re: Amended 2011 Section 702 Certifications)
- FISC Opinion (Sept. 25, 2012)
- FISC Opinion (Apr. 26, 2017)
- NSA Section 702 Targeting Procedures
- NSA Section 702 Minimization Procedures
- PCLOB, Recommendations Assessment Reports
- ODNI, Statistical Transparency Reports Regarding the Use of National Security Authorities
- Executive Office of the President of the United States, The Comprehensive National Cybersecurity Initiative
- U.S. Dep't of Homeland Security, Privacy Impact Assessment for the Initiative Three Exercise (Mar. 18, 2010)

- OLC, Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection System (Einstein 2.0) to Protect Unclassified Computer Networks in the Executive Branch (Jan. 9, 2009)
- U.S. Dep't of Homeland Security, Privacy Impact Assessment for Einstein 3 – Accelerated (E3A) (Apr. 19, 2013)
- U.S. Dep't of Homeland Security, Privacy Impact Assessment for Einstein 2 (May 19, 2008)

INTERROGATORY NO. 20:

Please state the basis of Plaintiff's allegations, in paragraphs 65 and 66 of the Amended Complaint, that in conducting Upstream surveillance "the government's aim is to 'comprehensively' … obtain communications to, from, and about targets scattered around the world," and that "the government is interested in obtaining, with a high degree of confidence, all international communications to, from, or about its targets."

RESPONSE TO INTERROGATORY NO. 20:

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is duplicative of other written discovery propounded by Defendants. Plaintiff also objects that this Interrogatory is improperly compound in that it contains multiple subparts.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows.

The PCLOB has described the use of Upstream surveillance to collect "about" communications as "an inevitable byproduct of the government's efforts to comprehensively acquire communications that are sent to or from its targets." PCLOB Report 10. And it has said

about Upstream surveillance more generally that this method's "success . . . depends on collection devices that can *reliably* acquire data packets associated with the proper communications." *Id.* at 143 (emphasis added); *see also* PCLOB, Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 26:15–18 (Mar. 19, 2014) (statement of Robert Litt, General Counsel, ODNI).

SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 20:

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement as discovery in this case continues, Plaintiff supplements its response as follows:

The bases for Plaintiff's allegations also include the following:

- [*Redacted*], No. [Redacted], 2011 WL 10945618 (FISC Oct. 3, 2011)
- PCLOB Report and official government sources concerning Upstream surveillance cited therein
- PCLOB, Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (Mar. 19, 2014)
- PCLOB, Public Hearing Regarding Consideration of Recommendations for Change: The Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act (Nov. 4, 2013)
- The document attached as Exhibit A to Plaintiff's First Set of Requests for Admission, "Why are we interested in HTTP?"
- Glenn Greenwald, *Xkeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet'*, The Guardian, July 31, 2013 (and associated documents).

- Julia Angwin & Jeff Larson, *New Snowden Documents Reveal Secret Memos Expanding Spying*, ProPublica (June 4, 2015) (and associated documents)
- Julia Angwin et al., *AT&T Helped U.S. Spy on Internet on Vast Scale*, N.Y. Times, Aug. 15, 2015 (and associated documents)
- Julia Angwin et al., *NSA Spying Relies on AT&T's 'Extreme Willingness to Help'*, ProPublica, Aug. 15, 2015 (and associated documents)
- Jeff Larson et al., *A Trail of Evidence Leading to AT&T's Partnership with the NSA*, ProPublica, Aug. 15, 2015 (and associated documents)
- Charlie Savage, *Power Wars* (2015)
- Charlie Savage, *N.S.A. Said to Search Content of Messages to and from U.S.*, N.Y. Times, Aug. 8, 2013
- Glenn Greenwald, *No Place to Hide* (2014)

Dated: April 17, 2018

/s/Ashley Gorski

Ashley Gorski
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
agorski@aclu.org

Counsel for Plaintiff Wikimedia Foundation, Inc.

SUPPLEMENTAL EXHIBIT C

Foreign Country, Territory, or Region	Number of HTTP Requests to Wikimedia's Servers in the United States from August 1, 2017 to January 31, 2018
Afghanistan	821,201
Åland	378
Albania	51,889
Algeria	843,262
Andorra	2,992
Angola	725,015
Anguilla	64,496
Antigua and Barbuda	725,010
Argentina	144,245,201
Armenia	167,659
Aruba	1,313,447
Australia	280,363,407
Austria	1,370,265
Azerbaijan	889,617
Bahamas	2,846,518
Bahrain	53,444
Bangladesh	26,717,162
Barbados	2,921,683
Belarus	489,593
Belgium	2,627,346
Belize	1,081,373

Benin	159,654
Bermuda	1,003,422
Bhutan	718,888
Bolivia	16,027,273
Bonaire, Sint Eustatius, and Saba	288,802
Bosnia and Herzegovina	36,230
Botswana	15,182
Brazil	743,523,019
British Indian Ocean Territory	143
British Virgin Islands	269,290
Brunei	1,434,086
Bulgaria	158,583
Burkina Faso	476,477
Burundi	186,611
Cabo Verde	5,301
Cambodia	9,423,280
Cameroon	828,395
Canada	626,430,503
Cayman Islands	1,266,819
Central African Republic	6,531
Chad	199,040
Chile	74,786,914
China	1,887,127,378

Christmas Island	8,375
Cocos [Keeling] Islands	923
Colombia	121,075,673
Comoros	3,666
Congo	1,074,674
Cook Islands	46,884
Costa Rica	22,372,501
Croatia	96,896
Cuba	719,445
Curaçao	2,678,493
Cyprus	124,788
Czechia	722,782
Denmark	215,876
Djibouti	20,527
Dominica	103,744
Dominican Republic	30,822,853
East Timor	181,512
Ecuador	55,544,542
Egypt	331,832
El Salvador	9,873,835
Equatorial Guinea	4,439
Eritrea	523
Estonia	66,476

Ethiopia	644,743
Falkland Islands	189
Faroe Islands	841
Federated States of Micronesia	64,610
Fiji	954,395
Finland	4,776,759
France	5,203,094
French Guiana	369,332
French Polynesia	895,747
French Southern Territories	7
Gabon	111,299
Gambia	38,860
Georgia	152,626
Germany	29,673,372
Ghana	290,814
Gibraltar	1,286
Greece	146,110
Greenland	600,633
Grenada	714,389
Guadeloupe	1,078,725
Guatemala	14,782,703
Guernsey	1,147
Guinea	329,981

Guinea-Bissau	19,274
Guyana	1,995,531
Haiti	1,799,389
Hashemite Kingdom of Jordan	748,358
Honduras	10,918,870
Hong Kong	132,445,801
Hungary	240,405
Iceland	26,267
India	262,028,913
Indonesia	454,933,133
Iran	33,154,224
Iraq	736,244
Ireland	593,762,872
Isle of Man	1,492
Israel	1,702,244
Italy	5,751,959
Ivory Coast	26,827
Jamaica	6,257,705
Japan	626,903,248
Jersey	5,088
Kazakhstan	233,815
Kenya	325,857
Kiribati	11,431

Kosovo	2,063
Kuwait	115,962
Kyrgyzstan	129,540
Laos	2,771,786
Latvia	67,497
Lebanon	226,570
Lesotho	91,060
Liberia	170,511
Libya	93,489
Liechtenstein	1,340
Luxembourg	40,681
Macao	4,414,341
Macedonia	30,060
Madagascar	211,134
Malawi	53,964
Malaysia	85,171,046
Maldives	2,314,246
Mali	169,424
Malta	47,636
Marshall Islands	38,106
Martinique	2,889,796
Mauritania	43,870
Mauritius	51,118

Mayotte	1,032
Mexico	276,945,398
Monaco	3,871
Mongolia	3,098,609
Montenegro	36,032
Montserrat	28,283
Morocco	495,003
Mozambique	110,182
Myanmar [Burma]	3,574,699
Namibia	15,794
Nauru	9,882
Nepal	14,121,673
Netherlands	38,092,032
New Caledonia	841,889
New Zealand	52,447,130
Nicaragua	8,800,538
Niger	59,676
Nigeria	523,467
Niue	4,402
Norfolk Island	4,200
North Korea	4,524
Norway	1,177,129
Oman	66,102

Pakistan	10,812,865
Palau	50,597
Palestine	157,595
Panama	19,029,566
Papua New Guinea	335,250
Paraguay	9,064,249
Peru	24,219,191
Philippines	89,704,175
Pitcairn Islands	36
Poland	2,958,397
Portugal	147,617
Qatar	156,184
Republic of Korea	690,307,638
Republic of Lithuania	69,788
Republic of Moldova	101,328
Republic of the Congo	52,530
Romania	393,888
Russia	2,680,016
Rwanda	414,825
Réunion	43,662
Saint Helena	38
Saint Kitts and Nevis	26,495
Saint Lucia	645,483

Saint Martin	101,279
Saint Pierre and Miquelon	29,128
Saint Vincent and the Grenadines	501,327
Saint-Barthélemy	3,287
Samoa	32,278
San Marino	272
Saudi Arabia	422,297
Senegal	122,076
Serbia	146,019
Seychelles	6,810
Sierra Leone	173,742
Singapore	189,603,688
Sint Maarten	375,159
Slovak Republic	4,858
Slovakia	95,273
Slovenia	26,343
Solomon Islands	40,868
Somalia	93,633
South Africa	473,077
South Georgia and the South Sandwich Islands	123
South Sudan	220,658
Spain	1,035,451
Sri Lanka	510,052

St Kitts and Nevis	324,512
Sudan	193,786
Suriname	1,613,129
Svalbard and Jan Mayen	73
Swaziland	110,645
Sweden	774,442
Switzerland	1,647,426
Syria	282,939
São Tomé and Príncipe	1,157
Taiwan	119,710,225
Tajikistan	334,945
Tanzania	617,298
Thailand	114,379,182
Togo	71,240
Tokelau	403
Tonga	30,399
Trinidad and Tobago	8,100,970
Tunisia	200,575
Turkey	28,568,637
Turkmenistan	38,007
Turks and Caicos Islands	564,567
Tuvalu	1,542
Uganda	1,741,953

Ukraine	2,377,191
United Arab Emirates	762,824
United Kingdom	15,128,140
Uruguay	9,577,567
Uzbekistan	268,916
Vanuatu	72,277
Vatican City	77
Venezuela	64,068,797
Vietnam	417,965,885
Wallis and Futuna	12,486
Western Sahara	10
Yemen	139,189
Zambia	714,196
Zimbabwe	961,529

SUPPLEMENTAL EXHIBIT D

Foreign Country, Territory, or Region	Number of HTTPS Requests to Wikimedia's Servers in the United States from August 1, 2017 to January 31, 2018
Afghanistan	20,604,532
Åland	133,943
Albania	9,643,581
Algeria	128,780,026
Andorra	265,822
Angola	113,578,445
Anguilla	2,217,119
Antigua and Barbuda	34,519,166
Argentina	13,052,041,069
Armenia	16,619,809
Aruba	46,034,224
Australia	19,425,507,629
Austria	43,074,736
Azerbaijan	92,885,398
Bahamas	112,093,153
Bahrain	6,954,957
Bangladesh	2,385,092,865
Barbados	115,182,398
Belarus	81,967,203
Belgium	60,091,900
Belize	51,618,265
Benin	23,946,277
Bermuda	40,147,959
Bhutan	36,331,354

Bolivia	1,404,857,896
Bonaire, Sint Eustatius, and Saba	10,085,028
Bosnia and Herzegovina	7,020,177
Botswana	2,451,091
Brazil	31,015,286,204
British Indian Ocean Territory	12,169
British Virgin Islands	4,623,366
Brunei	156,296,973
Bulgaria	30,331,597
Burkina Faso	82,427,481
Burundi	30,241,949
Cabo Verde	920,646
Cambodia	369,780,518
Cameroon	133,484,746
Canada	36,379,477,322
Cayman Islands	39,135,595
Central African Republic	1,415,519
Chad	34,068,856
Chile	6,726,153,714
China	7,835,059,394
Christmas Island	352,364
Cocos [Keeling] Islands	115,575
Colombia	11,515,675,774
Comoros	1,317,537
Congo	228,406,703
Cook Islands	2,939,189

Costa Rica	1,262,430,752
Croatia	16,927,085
Cuba	186,179,730
Curaçao	59,625,943
Cyprus	6,689,187
Czechia	58,231,479
Denmark	38,271,882
Djibouti	2,140,379
Dominica	8,080,763
Dominican Republic	2,151,854,032
East Timor	24,375,421
Ecuador	3,860,446,842
Egypt	57,100,043
El Salvador	882,209,181
Equatorial Guinea	680,068
Eritrea	60,304
Estonia	8,603,956
Ethiopia	84,571,842
Falkland Islands	18,642
Faroe Islands	158,452
Federated States of Micronesia	4,517,004
Fiji	77,928,890
Finland	29,158,348
France	358,230,836
French Guiana	19,324,082
French Polynesia	80,847,556

French Southern Territories	736
Gabon	27,078,961
Gambia	6,384,517
Georgia	22,408,026
Germany	562,211,287
Ghana	46,368,618
Gibraltar	306,873
Greece	46,363,715
Greenland	14,325,826
Grenada	27,344,536
Guadeloupe	66,885,212
Guatemala	1,472,820,804
Guernsey	334,080
Guinea	83,260,527
Guinea-Bissau	4,255,517
Guyana	79,823,616
Haiti	265,132,981
Hashemite Kingdom of Jordan	91,259,008
Honduras	744,069,894
Hong Kong	8,716,103,273
Hungary	47,081,457
Iceland	2,711,278
India	3,165,955,918
Indonesia	13,116,466,025
Iran	87,510,049
Iraq	24,405,997

Ireland	2,112,117,966
Isle of Man	341,100
Israel	62,141,461
Italy	210,385,545
Ivory Coast	3,970,928
Jamaica	395,757,541
Japan	85,441,052,143
Jersey	345,920
Kazakhstan	44,137,526
Kenya	49,280,668
Kiribati	1,689,164
Kosovo	342,323
Kuwait	14,247,593
Kyrgyzstan	31,333,488
Laos	109,472,472
Latvia	9,104,225
Lebanon	13,599,863
Lesotho	13,499,426
Liberia	26,031,402
Libya	9,195,709
Liechtenstein	215,673
Luxembourg	5,639,047
Macao	411,561,258
Macedonia	5,123,868
Madagascar	58,417,988
Malawi	7,613,927

Malaysia	6,437,106,376
Maldives	94,625,241
Mali	37,296,988
Malta	2,509,967
Marshall Islands	2,897,907
Martinique	83,396,604
Mauritania	7,882,681
Mauritius	2,468,551
Mayotte	193,971
Mexico	26,039,248,714
Monaco	541,934
Mongolia	301,320,409
Montenegro	2,819,788
Montserrat	1,252,999
Morocco	76,616,817
Mozambique	22,792,076
Myanmar [Burma]	384,217,247
Namibia	1,070,964
Nauru	538,677
Nepal	598,746,931
Netherlands	204,649,528
New Caledonia	102,524,542
New Zealand	3,539,655,892
Nicaragua	456,108,803
Niger	12,480,647
Nigeria	50,500,001

Niue	225,126
Norfolk Island	235,514
North Korea	887,377
Norway	40,036,961
Oman	6,073,423
Pakistan	318,156,164
Palau	2,828,940
Palestine	11,032,480
Panama	1,189,381,456
Papua New Guinea	48,345,831
Paraguay	752,603,128
Peru	7,030,573,552
Philippines	9,277,043,820
Pitcairn Islands	23,977
Poland	228,061,723
Portugal	26,235,675
Qatar	14,554,687
Republic of Korea	8,320,136,352
Republic of Lithuania	11,873,194
Republic of Moldova	12,242,253
Republic of the Congo	12,001,830
Romania	100,552,982
Russia	288,064,755
Rwanda	41,922,847
Réunion	2,043,341
Saint Helena	16,961

Saint Kitts and Nevis	1,583,317
Saint Lucia	37,677,429
Saint Martin	4,577,110
Saint Pierre and Miquelon	5,106,171
Saint Vincent and the Grenadines	20,676,869
Saint-Barthélemy	317,643
Samoa	3,592,302
San Marino	42,125
Saudi Arabia	39,968,209
Senegal	22,533,953
Serbia	47,477,541
Seychelles	620,663
Sierra Leone	26,258,425
Singapore	5,131,135,255
Sint Maarten	11,305,651
Slovak Republic	1,121,120
Slovakia	16,705,364
Slovenia	5,575,086
Solomon Islands	8,907,274
Somalia	15,262,543
South Africa	34,949,275
South Georgia and the South Sandwich Islands	33,982
South Sudan	15,109,935
Spain	149,596,780
Sri Lanka	68,750,415
St Kitts and Nevis	13,753,545

Sudan	22,173,374
Suriname	78,396,254
Svalbard and Jan Mayen	1,408
Swaziland	15,120,981
Sweden	53,487,983
Switzerland	63,031,700
Syria	36,608,575
São Tomé and Príncipe	364,059
Taiwan	17,479,596,696
Tajikistan	67,222,492
Tanzania	58,174,269
Thailand	7,935,948,956
Togo	15,386,691
Tokelau	33,274
Tonga	3,723,043
Trinidad and Tobago	338,216,935
Tunisia	34,125,021
Turkey	1,118,611,571
Turkmenistan	1,258,697
Turks and Caicos Islands	8,998,062
Tuvalu	153,174
Uganda	190,307,650
Ukraine	520,208,217
United Arab Emirates	58,227,626
United Kingdom	574,948,730
Uruguay	1,374,562,931

Uzbekistan	32,395,981
Vanuatu	9,045,979
Vatican City	15,768
Venezuela	5,382,496,004
Vietnam	6,578,718,936
Wallis and Futuna	1,360,077
Western Sahara	3,664
Yemen	7,653,920
Zambia	94,948,340
Zimbabwe	61,649,107

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix BB

This document was also filed as ECF No. 164-7 and can be found in this Joint Appendix at JA0861.

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix C

Next Generation Network, and Transoceanic Subsea Cable Updates

Presented by:
City of Virginia Beach
Department of Information Technology
October 4, 2017

Strategic Planning & Partnerships

- **Master Technology Plan**
  - A roadmap for how the IT department will partner with other city departments to implement the right technologies needed for long-term business success.
  - Includes four major pillars that all IT department initiatives support:
    1. Transforming service delivery
    2. Building better business solutions
    3. Strengthening IT governance
    4. Improving infrastructure and operations
  - Next Generation Network (NGN) – Initiative I-1
    - The "Improving infrastructure and operations" pillar included a recommendation to explore ways to create a Next Generation Network.
      - Documents the city's progress in creating the NGN
      - Assesses the city's need and market for future NGN capabilities
      - Provides strategic and technical recommendations for achieving the city's goals related to broadband infrastructure and operations
- **Broadband Resolution**
  - Adopted by City Council in March 2015
  - Charged staff to explore and create opportunities to leverage NGN investments made by the city and VBCPS to advance high-speed broadband across the region.
  - Broad Band Task Force (2015-2016)

Strategic Planning & Partnerships for Next Generation Network

➢ CVB Broadband Task Force Goals

- Purpose and Objective: Build a Next Generation Network that:
  - Provides excellent city services
  - Reduce digital divide for families and businesses
  - Grow our economy
  - Support 21st century jobs
  - Expand fiber network to connect additional off-campus locations to municipal campus and create network redundancy
  - Leverage NGN for the following:
    - Expand educational opportunities
    - Contribute to regional opportunities
    - Utilize “Dig Once” strategy for road and utility projects to include fiber and conduit

➢ CVB Broadband Strategy

- Support city council goal of a financially sustainable city that provides excellent services by making strategic investments in NGN and Transoceanic Cable.
- Create a Middle Mile infrastructure that enhances opportunities in economic development, education, and regional connectivity.
- Enhance the build out new businesses and growth areas (e.g., Biomed) and make business parks fiber ready to attract new businesses.
- Lease excess capacity (dark fiber) vs. providing lit services to create opportunities for expanding internal government services.
- Create internal and external partnerships to take advantage of Transoceanic Cable opportunities.

➢ Regional CIO Broadband Task Force

- City Manager and CIO met regularly with regional City Managers to discuss regional broadband opportunities.
- Collaborated with other municipalities to explore potential regional broadband opportunities.
- Shared education of emerging clusters.

➢ City Manager’s Directive

- Directive to include fiber expansion in all Public Works construction projects.

Strategic Planning & Partnerships for Next Generation Network

Broadband White Paper

- A High-Speed Broadband White Paper was developed to:
  - Provide a history of broadband on a local, state and national level
  - Identify the current trends in broadband
  - Provide an overview of the laws surrounding broadband
  - Support the city's broadband vision for Virginia Beach, as outlined in the Envision Virginia Beach 2040 report:
    - "Citizens, businesses and visitors have access to advanced broadband technologies that efficiently and effectively supports regional interconnectivity as well as global commerce."
  - Meet market demand

Business Case

- A business case was developed to provide a financial analysis and comparison between leased network fiber and City-owned network fiber.
- This document assisted city leadership and stakeholders with determining if the project would provide value to the enterprise.
- The document also served to justify the capital outlay for the project.
- Stakeholders from various departments were involved with the assessment of current and future bandwith needs.
- Costs and savings were identified and entered into a ROI calculator to provide the quantitative benefits of implementing fiber.

Formalized Process for Fiber Provisioning Management

- Document that describes the processes that will be required for building out the fiber infrastructure
  1. Provisioning fiber to a building location that is not part of the NGN
  2. Provisioning fiber to a building that is being newly constructed by Public Works
  3. Provisioning fiber for road, sidewalk and Intelligent Traffic System projects
  4. Repairing a confirmed fiber service outage
  5. Repairing damaged NGN network infrastructure

Strategic Planning & Partnerships for Next Generation Network

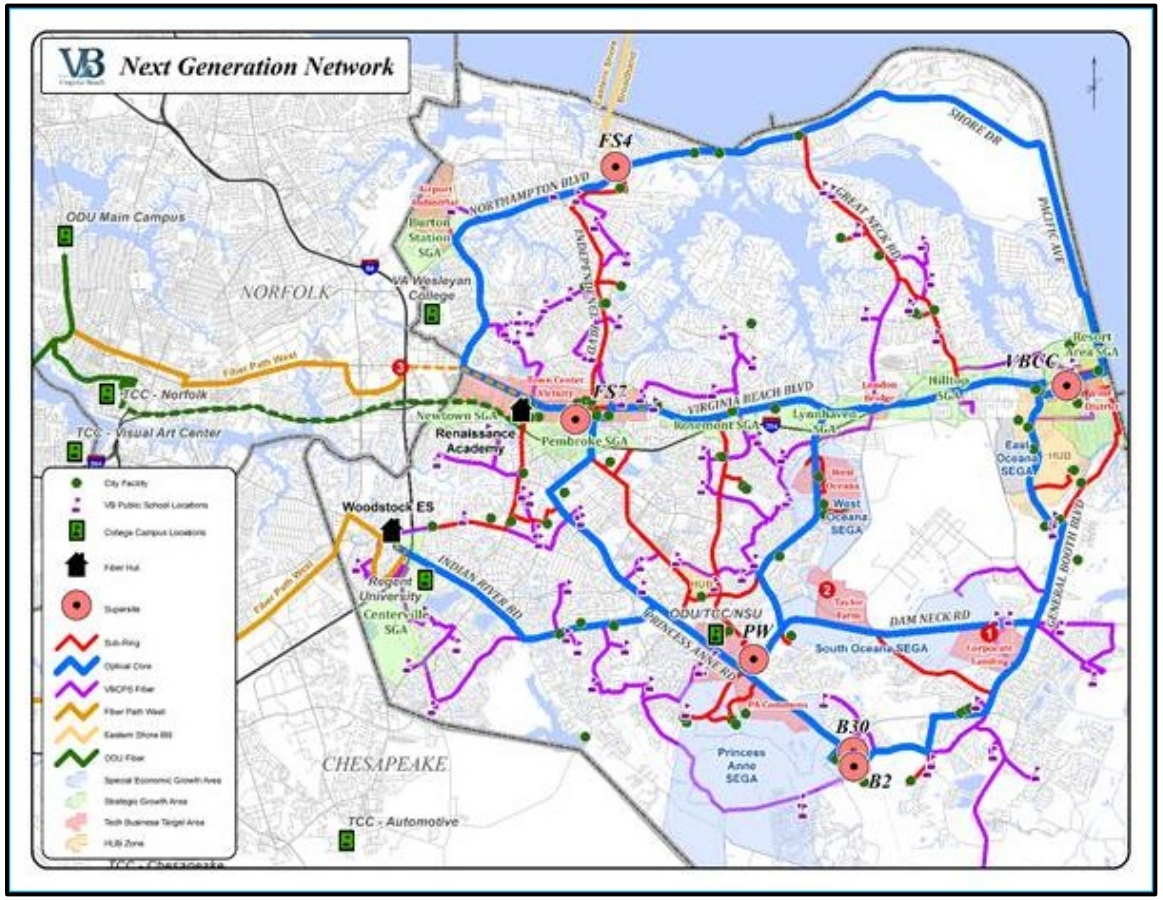
- **CBG Communications**
  - Telecommunications and cable television consulting firm that conducted both residential and business broadband surveys to gauge the community's need for broadband services.

- **3U Technologies**
  - International business consulting, project management and engineering services firm that developed a Proposal for Support of Submarine Cable Landing

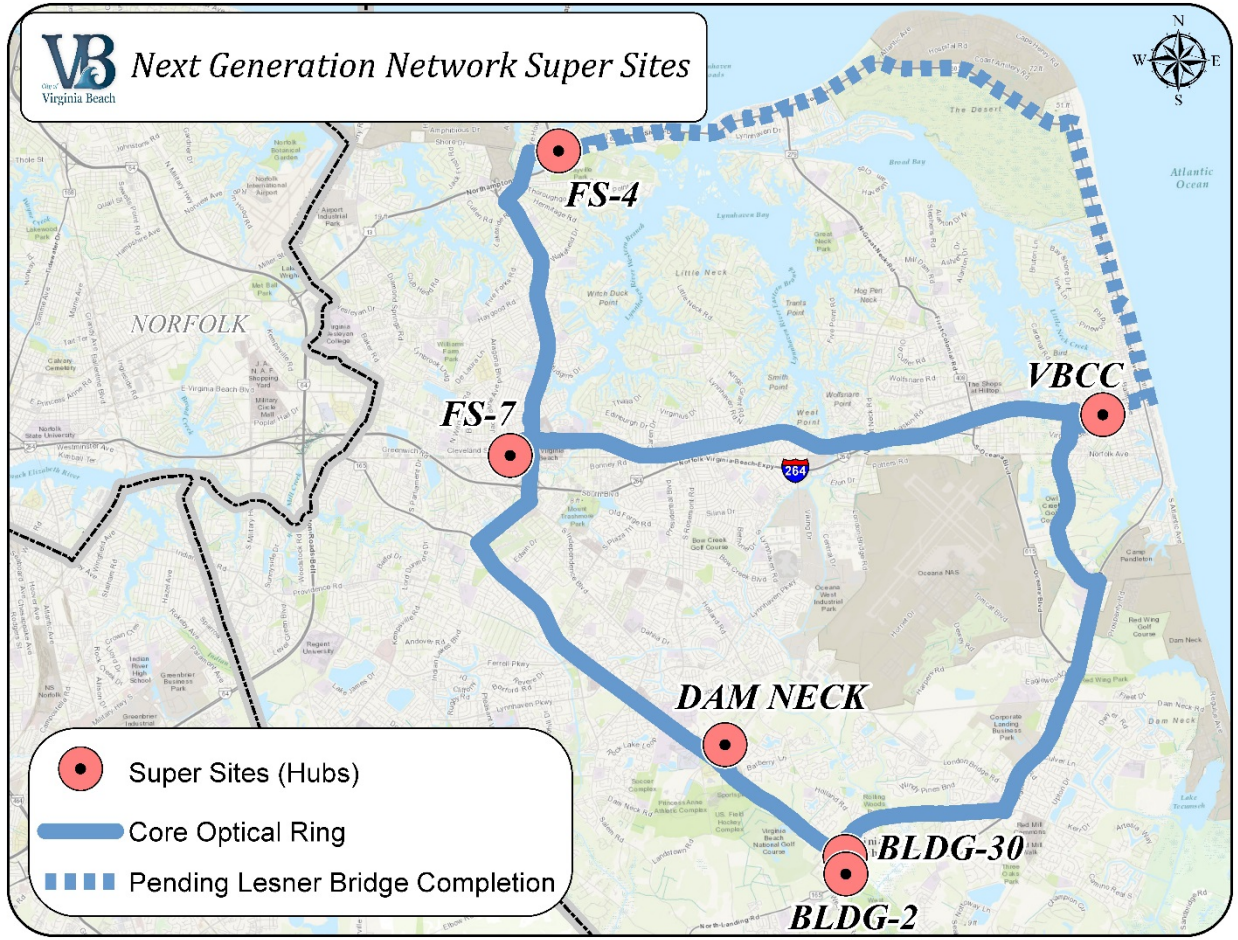
- **CTC Technology & Energy**
  - An independent communications and IT engineering consulting firm that assisted with developing middle mile leasing strategies.

Next Generation Network Buildout

- City of Virginia Beach invested $4.1 million in their FY 15 budget
- Leveraged the existing infrastructure to buildout and connect facilities
- Mapped strategic routes to 60 connected locations
  - Designed for future economic opportunities
  - Taking into consideration the proximity of corporate parks
  - City road projects will include conduit/fiber
  - Put infrastructure in place to support NGN



Next Generation Network

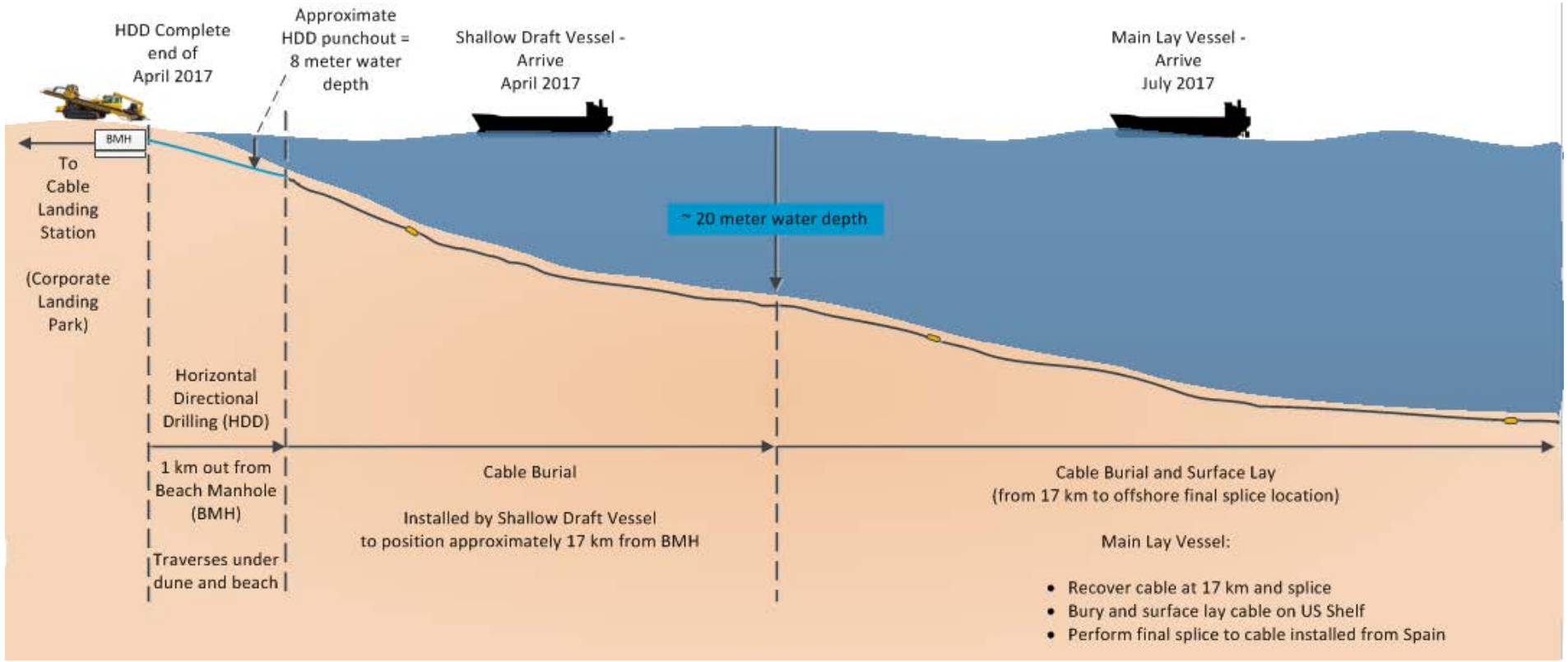


- Total of 6 Optical/Super Sites (Phase 0) and
- 54 Remote Locations (Phases 1 through 4)
- Construction Completion Dates:
  - Phase 0 – 06/24/2016
  - Phase 1 – 10/18/2016
  - Phase 2 – 04/07/2017
  - Phase 3 – 04/28/2017
  - Phase 4 – 06/15/2017
- NGN Go Live Date – Dec, 2017

Transoceanic Subsea Fiber Cables

MAREA Cable – From beach to manhole

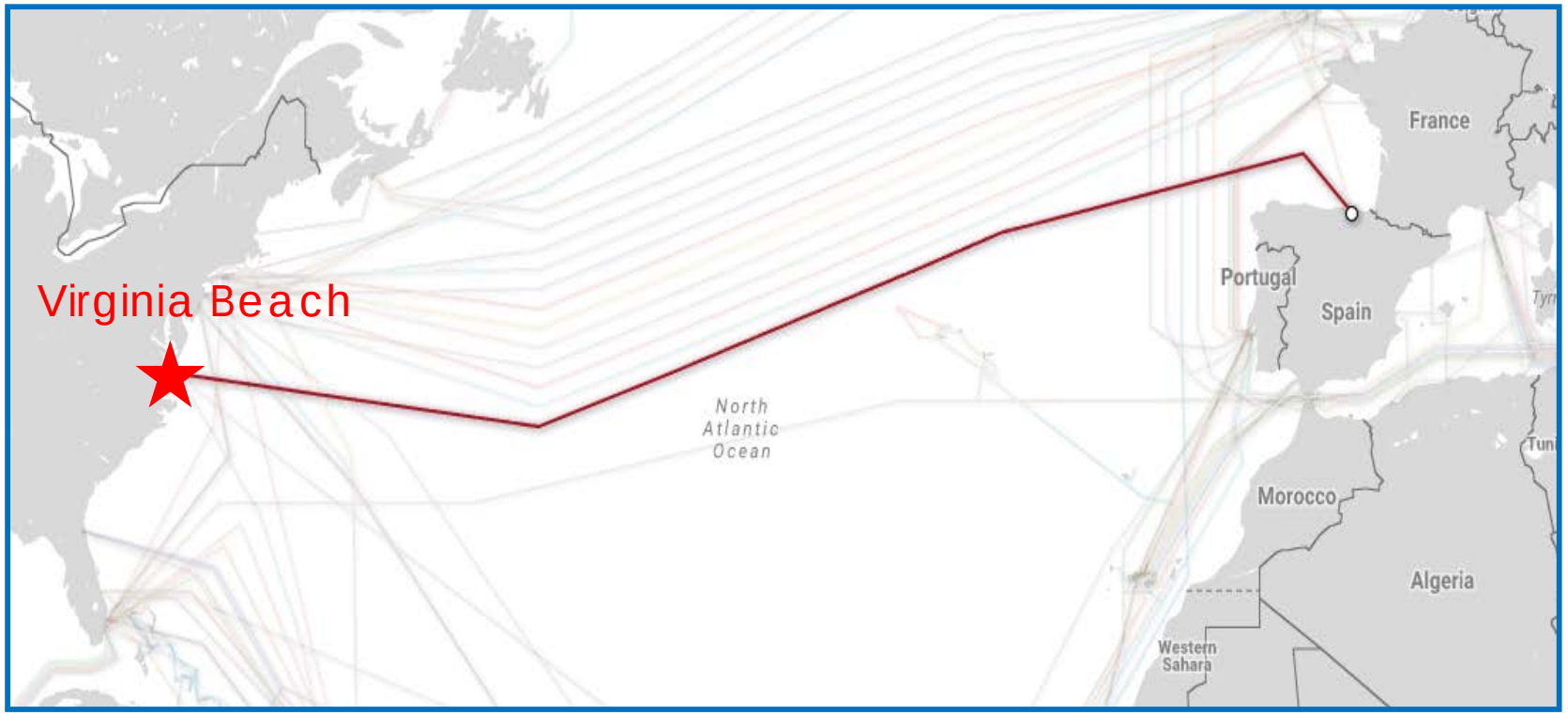
- **Oceanic** Infrastructure connection of subsea cable
  - Will connect sub-sea cable to off-shore duct duckbill flap (4 conduits for the MAREA/BRUSA beach manhole)
  - Clear in (ships check in port)
    - (shallow draft vessel) April 7 – 14, 2017
    - (main lay vessel) July 19 – Aug 15, 2017
  - Operational Period
    - (shallow draft vessel) April 7 – 14, 2017
    - (main lay vessel) July 19 – Aug 10, 2017



Transoceanic Subsea Fiber Cables

MAREA

Virginia Beach to Bilbao, Spain



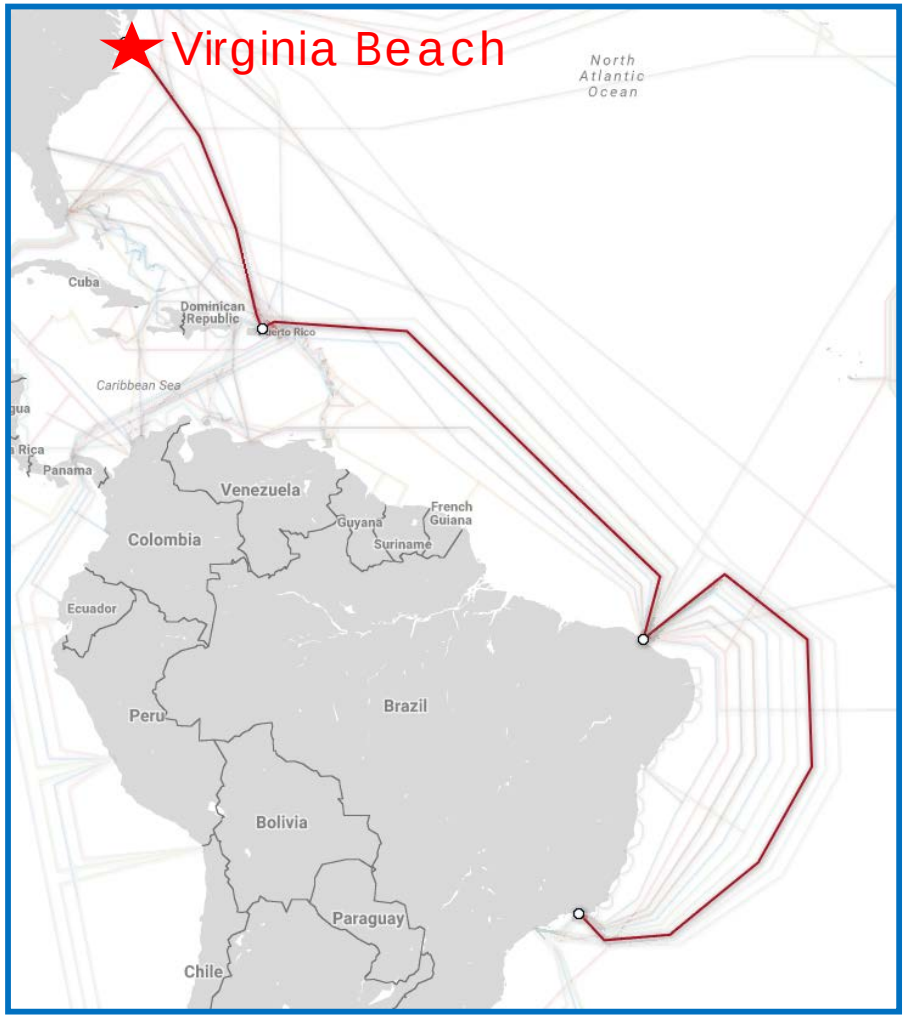
- Led by **Microsoft and Facebook, MAREA will be the highest-capacity subsea cable to ever cross the Atlantic**
- The new **6,600 km submarine cable system** will connect **Virginia Beach, Virginia to Bilbao, Spain**
- This new southern **route will provide greater diversity of connections & enhanced reliability** for customers
- Optimal connectivity to data centers on the East Coast
- Highest capacity cable to ever cross the Atlantic Ocean at 160 Tb/s

System Testing: **October 2017**
System Operational: **November/December 2017**

Transoceanic Subsea Fiber Cables

BRUSA

Virginia Beach to San Juan, Puerto Rico and Rio de Janeiro Brazil

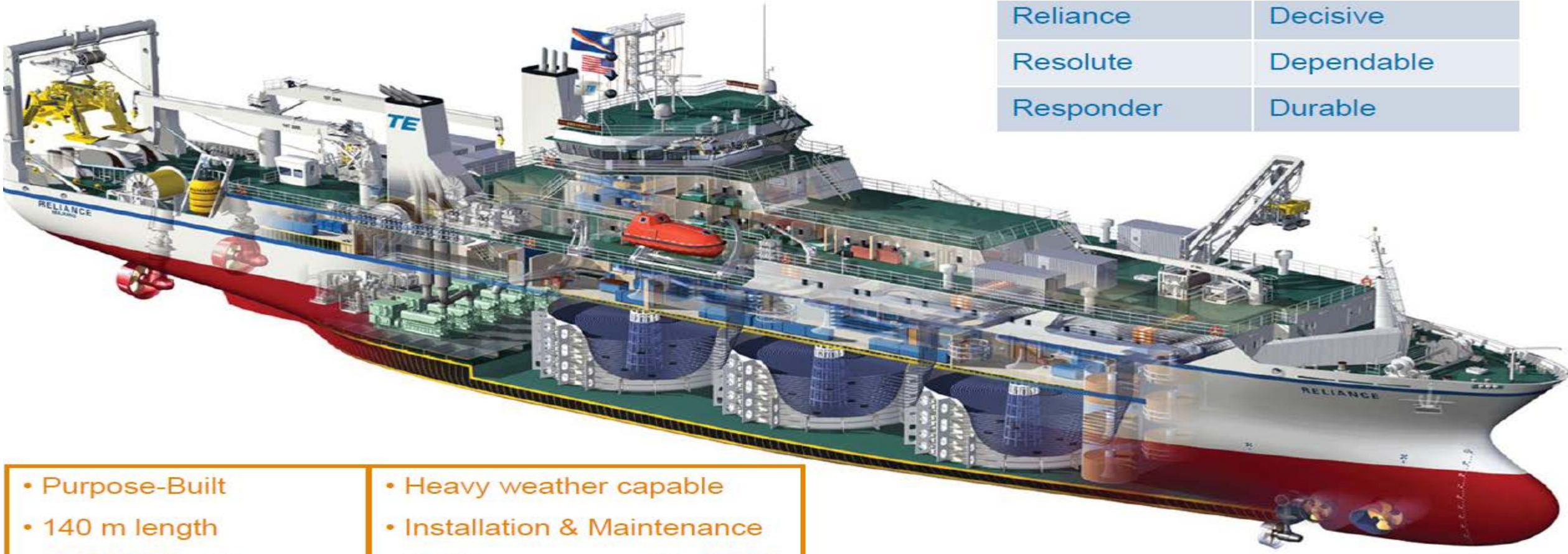


BRUSA Cable and Conduit Installation: **June 2018**
(dates per Telefonica)

- Led by Telxius Cable USA
- Nearly **11,000 km in length** linking **Rio de Janeiro** and **Fortaleza** (Brazil) with **San Juan** (Puerto Rico) and **Virginia Beach** (USA)
- Leading edge technology supporting **ultrafast transmission capacity**
- Increased end-to-end connectivity and the **availability of ultra high-speed broadband services**
- This new **infrastructure will address the exponential growth of data transmission** generated by its B2B customers, telecom operators, OTT players and end-consumers
- Will **improve communication reliability and deliver enhanced resilience by increasing the number of USA landing points**
- Will also provide the **lowest latency communication links between the two largest economies in the region, Brazil and USA**

Transoceanic Subsea Fiber Cables – Main Vessel

Reliance	Decisive
Resolute	Dependable
Responder	Durable

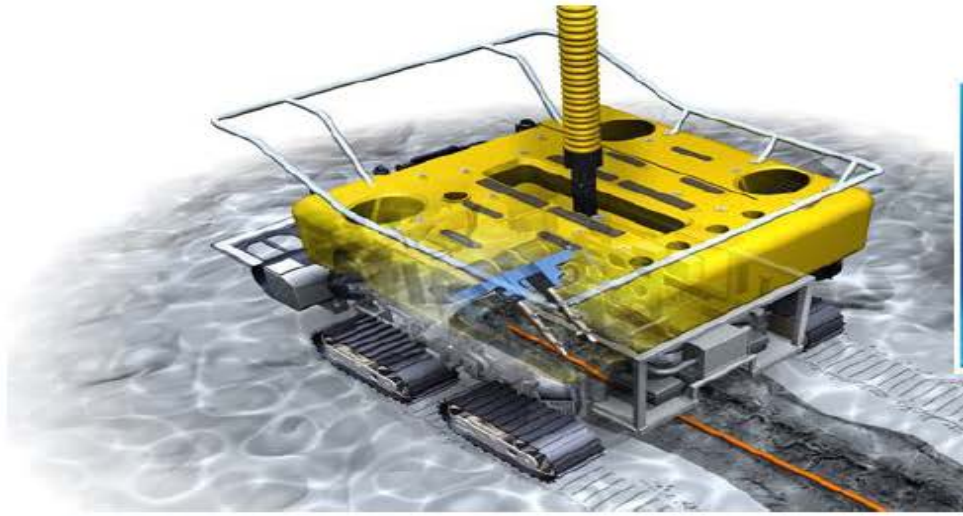


- Purpose-Built
- 140 m length
- 5,500 MT cable cap.
- 84 persons
- 60+ days endurance

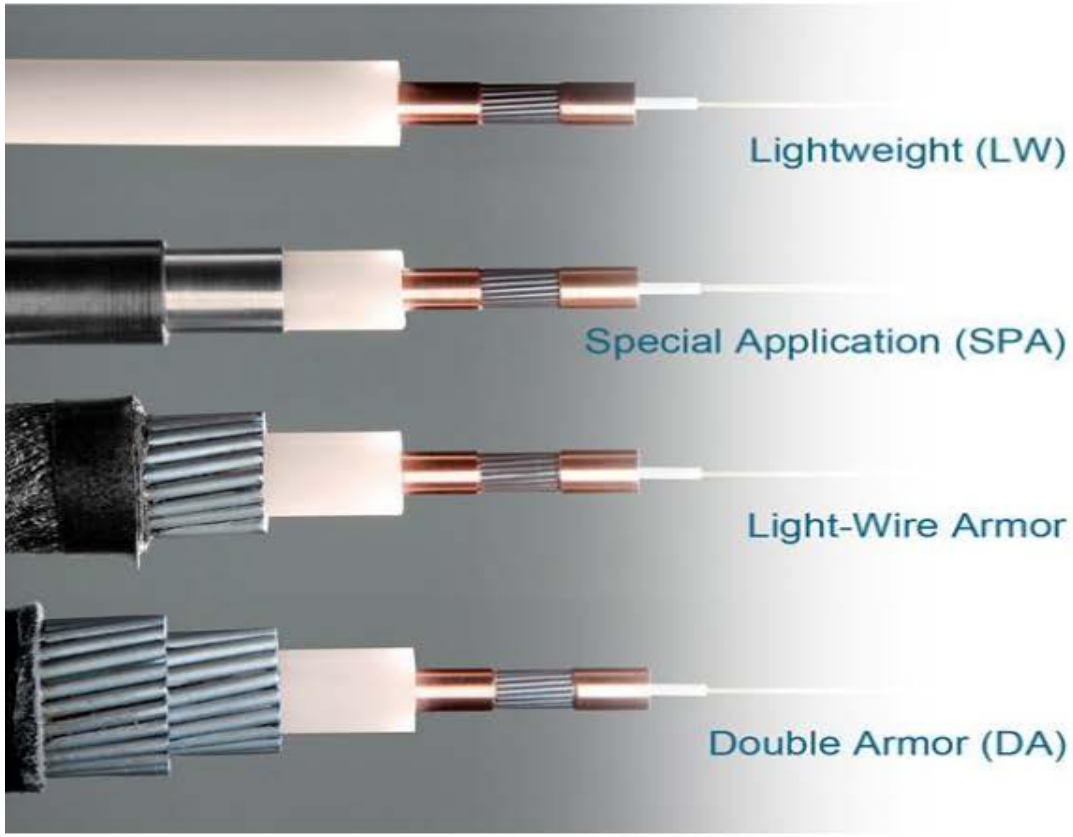
- Heavy weather capable
- Installation & Maintenance
- Highly maneuverable (DP2)
- Plow & ROV equipped
- 60 MT A-Frame

JA1874

Transoceanic Subsea Fiber Cables
Remotely Operated Vehicles (ROV)

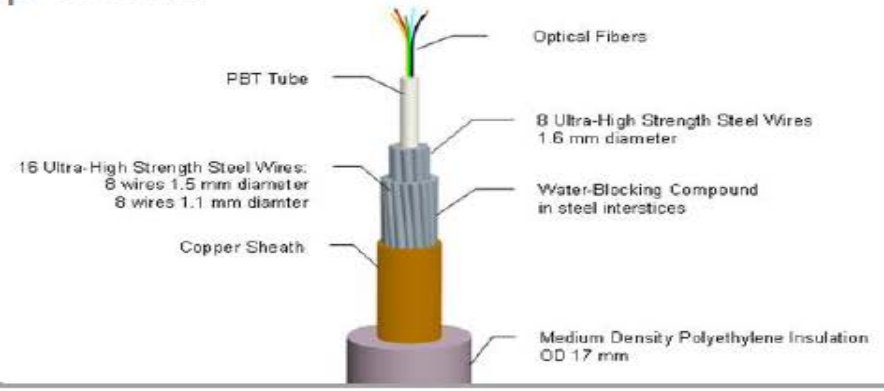


Transoceanic Subsea Fiber Cables

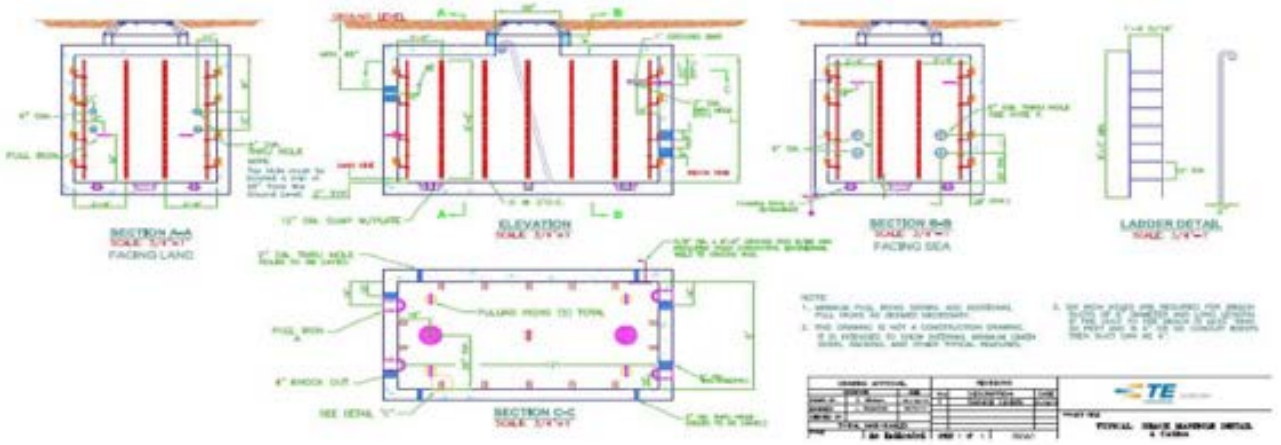


Undersea cables…

- protect optical fibers and an electrical conductor to carry telephone, internet & data communications traffic at ~2.5 TB/second;
- are built durable, yet flexible, to support system deployment, recovery, repair & re-deployment;
- are inert in the marine environment;
- offer various levels of protection from subsea conditions and external aggression, such as: rocky terrain, fishing activity, high risk of abrasion or crushing (e.g., anchoring), and the deep ocean.



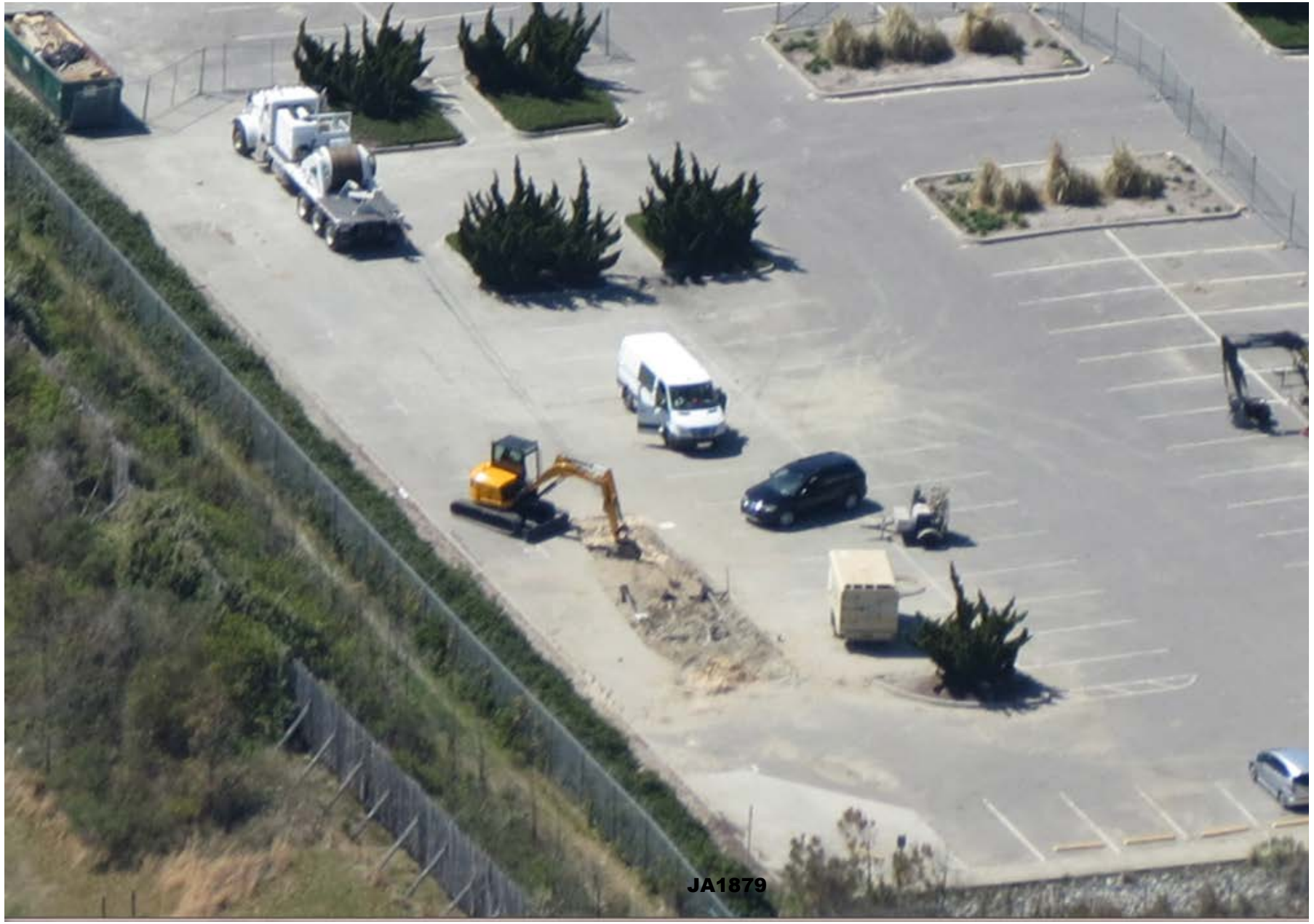
Transatlantic Subsea Fiber Cables



- **2 BMH's planned**
- **Typical BMH Design: 12' L x 6' W x 7' H**
- **Buried (below ground level) within the parking lot, with corresponding buried ocean ground bed anodes**
- **No Significant impact to the long-term functionality of the parking lot**

Transoceanic Subsea Fiber Cables – Shallow Water Vessel

Transoceanic Subsea Fiber Cables – Landing Point, Camp Pendleton



Transatlantic Subsea Fiber Cables

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix DD

This document was also filed as ECF No. 168-27 and can be found in this Joint Appendix at JA2932.

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix EE

Application No. 24960/15

IN THE EUROPEAN COURT OF HUMAN RIGHTS

BETWEEN:

10 HUMAN RIGHTS ORGANISATIONS

Applicants

-and-

THE UNITED KINGDOM

Respondent

FURTHER OBSERVATIONS OF THE GOVERNMENT OF THE UNITED KINGDOM

I Introduction

1. By way of a letter dated 11 October 2016, enclosing the Applicants' further observations and claims for just satisfaction, the Court invited the Government's response to the claims for just satisfaction and any other observations the Government wish to make.

2. These further observations are submitted in response to that invitation by the Court. They also contain the Government's response to the Third Party interventions that have made in this case[1].

3. The Government has already submitted detailed Observations on Admissibility and the Merits addressing the Intelligence Sharing and s.8(4) regimes (referred to hereinafter as "the Observations"), and responding to the specific questions posed by the Court. The Government adopts, but does not repeat, those Observations and has sought to confine these further Observations to new points of substance which have

[1] Three such interventions have been made by Third Parties: (1) The European Network of National Human Rights Institutions ("ENNHRI"); (2) The Electronic Privacy Information Center and (3) Article 19.

been raised by the Applicants or the Intervenors. Where the substance of the interventions is already addressed in the Government's Observations, the Government cross-refers to the relevant paragraphs of the Observations, rather than repeating their substance. The Government uses the same terminology in this Response as is used in the glossary to its Observations.

I. RESPONSE TO 10 HUMAN RIGHTS FURTHER OBSERVATIONS

4. In common with the way in which the Applicant's have structured their further observations, the Government proposes to address the factual assertions which are now made about the two regimes (Part 1), before making a number of legal submissions in response to the Applicants' further observations (Part 2).

THE FACTS

The section 8(4) Regime – general observations

5. Although the Applicants have correctly moved away from characterising the s.8(4) regime as one of "mass surveillance", they nevertheless seek to portray it as a regime in which the totality of communications across entire networks are the subject of substantive and meaningful invasions of privacy in an arbitrary and disproportionate manner[2].

6. But that is to mis-characterise and over-simplify the process and ignores the surgical precision with which GCHQ does (and is legally obliged to) interrogate bulk data pursuant to its statutory powers.

7. Whilst the Security and Intelligence Agencies (SIAs) do intercept the entire contents of a bearer or bearers under the s.8(4) Regime, they only examine a tiny proportion of communications or communications data from those contents, having chosen to examine them, on the basis of statutory tests of purpose, and requirements of necessity and proportionality. This is focused intelligence gathering. Without this

[2] See, in particular §35-37 and 42-46 of the Applicants' further observations.

capability, much vital intelligence would not be available to the UK for legitimate public protection purposes.

8. As explained in detail in the Observations, the s.8(4) Regime operates in this way as a matter of practical necessity. For technical reasons, it is necessary to intercept the entire contents of a bearer, in order to extract even a single specific communication for examination from the bearer: Observations, §§1.31-1.34.

9. Such an act of interception is characterised by the Court as involving an interference with Article 8(1) ECHR. But in truth, it cannot involve a substantial invasion of individuals' privacy rights unless that communication is selected for examination: in other words, unless a human examines it, or may potentially examine it. The analysis of Article 8 rights must focus upon the stage at which a communication is selected for examination; not simply upon the act of interception in itself. If the analysis fails to do this, it will fail to grapple with the true nature of the s.8(4) Regime, how it works, and what activities it permits. And the position is no different, just because communications passing over a bearer may be held temporarily (often for fractions of a second) while they are electronically filtered and subjected to search terms, to determine whether they are selected for such examination.

10. Thus, what ultimately matters for privacy rights is not the mere fact that data are subject to bulk interception. What matters is the adequacy of the safeguards that either allow or prevent such data from being examined. The Government has set out in detail in its Observations the reasons why those safeguards are well sufficient to secure individuals' Article 8 rights, by reason of the statutory framework in RIPA, the Code, the internal safeguards of the Intelligence Services, the application of tests of necessity and proportionality, and the oversight of the IPT, ISC and Commissioner.

11. A regime that operates on the basis of strict controls governing the selection of data for examination, which limits the statutory purposes for which those data can be selected for examination, and which applies tests of necessity and proportionality to such selection, cannot contravene Article 8 ECHR, merely because at the initial stage

a large amount of data is intercepted. Otherwise, the Court's judgment in *Weber and Saravia v Germany* (app. 54934/00) ("*Weber*"), which established the legal requirements governing the interception of communications in this field, would have been wrongly decided.

12. In short, it is illegitimate to suggest that bulk interception itself inevitably entails a breach of Article 8 ECHR.

The Bulk Powers Review

13. The Independent Terrorism Legislation Reviewer has produced further important factual evidence about the Intelligence Services' bulk interception practices pursuant to the s.8(4) Regime, and the intelligence need for such bulk interception. See the Report of the Bulk Powers Review (David Anderson QC), August 2016 ("the Bulk Powers Review").

14. The Bulk Powers Review evaluated the operational case for various intelligence gathering powers, in the context of the Investigatory Powers Bill (which received Royal Assent on 29 November 2016 as the Investigatory Powers Act, though most of the Act is not yet in force), which is intended to provide a new statutory framework for such powers. One of the powers considered in the Review was bulk interception, i.e. interception currently conducted under the s.8(4) Regime.

15. The Bulk Powers Review provides a helpful summary of the way in which bulk interception under the s.8(4) Regime works at §§2.13-2.18, which emphasises the important distinction between the initial interception and filtering of communications, and their selection for potential examination, set out above:

"2.14 Bulk interception involves three stages, which may be called ***collection, filtering*** *and* ***selection for examination****.*

First stage: collection
2.15 GCHQ selects which bearers to access based on an assessment of the likely intelligence value of the communications they are carrying. GCHQ does not have the capacity, or legal authority, to access every bearer in the world. Instead it focuses its resources on those links that it assesses will be the most valuable. At any given time, GCHQ has access to only a tiny fraction of all the bearers in the world.

Second stage: filtering
2.16 GCHQ's processing systems operate on the bearers which it has chosen to access. A degree of filtering is then applied to the traffic on these bearers, designed to select communications of potential intelligence value. As a result of this filtering stage, the processing systems automatically discard a significant proportion of the communications on the targeted bearers.

Third stage: selection for examination
2.17 The remaining communications are then subjected to the application of queries, both simple and complex, to draw out communications of intelligence value. Examples of a simple query are searches against a "strong selector" such as a telephone number or email address. Complex queries combine a number of criteria, which may include weaker selectors but which in combination aim to reduce the odds of a false positive. Communications that do not match the chosen criteria are automatically discarded. The retained communications are available to analysts for possible examination.

2.18 The application of these queries may still leave too many items for analysts to examine, so GCHQ must then carry out a triage process to determine which will be of most use. The triage process means that the vast majority of all the items collected are never looked at by analysts…"

16. At §§2.19, the Review summarises the two major processes that GCHQ applies to bulk interception (i.e. the "strong selector" process and "complex query" process), observing that (i) the "strong selector" process is in effect a "targeted" process, not a "bulk" process at all, because the selectors used relate to individual targets; and (ii) the "complex query" process permits methods of analysis and selection not available with the "strong selector" process, but in no way permits staff to search through communications *"at will"*. It is *"closer to true bulk interception, since it involves the collection of unselected content and/or secondary data"*. But *"as with the [strong selector process], it remains the case that communications unlikely to be of intelligence value are discarded as soon as that becomes apparent"*.

17. At §2.20, David Anderson QC observes that he has "no reason to disagree" with the ISC's assessment that the s.8(4) Regime does not collect communications indiscriminately, and that *"only the communications of suspected criminals or national security targets are deliberately selected for examination"*.

18. Chapter 5 of the Bulk Powers Review assesses the utility of bulk interception, as carried out by GCHQ under the s.8(4) Regime. That assessment was undertaken on the basis of an intensive review of closed evidence: see §5.2:

"Cathryn McGahey QC and I have inspected a great deal of closed material concerning the value of bulk interception, including warrant renewal applications (which contain details of the use to which intelligence derived from bulk interception had been put) and explanations produced for the benefit of the ISC and the Review."

19. Points made in Chapter 5 include the following:

(1) Just under half of all GCHQ intelligence reporting is based on data obtained under bulk interception warrants. For counter-terrorism intelligence reporting, this figure rises to over half: §5.9.

(2) Targeted interception cannot be viewed as a generally viable substitute for bulk interception. Even where a "strong selector" is known (e.g. a telephone number or email address), it may in an overseas context very often be necessary to intercept in bulk in order to obtain information from that selector. A targeted warrant would very often not produce the same result. See §§5.24-5.33:

(i) The location of some targets may mean that targeted interception would not be practicable (e.g. the target in Syria).

(ii) Even in more favourable overseas locations, the cooperation of local CSPs in giving effect to a targeted warrant might not be forthcoming, or might be possible only after delays.

(iii) The fragmentary nature of global communications, involving the division of communications into packets, means that a targeted warrant would not, or would not necessarily, capture all the information that GCHQ needs.

(iv) The number of overseas targets could render such a regime prohibitively cumbersome.

(v) "Contact chaining"[3] on the basis of targeted interception is a valuable technique, but has limitations. It is dependent upon the Intelligence Agencies already knowing their initial subject of interest; new subjects of interest being in contact with the initial subject; and it being possible to serve a targeted interception warrant on new subjects. Those conditions will not always be satisfied, particularly where subjects of interest are overseas. Moreover, "contact chaining" may very well not work where

[3] That is, identifying terrorist connections through interrogation of data obtained through targeted means, in order to find additional contacts who use the same form of communication.

extremists use a variety of different communications methods in an effort to conceal their activities: §§5.28-5.33.

(3) Bulk acquisition of communications data may in some circumstances be an adequate alternative to bulk interception: but it would not be noticeably less intrusive and would have a disadvantage in terms of speed (and the need for cooperation from CSPs): §5.34.

(4) Similarly, human sources of intelligence may be unavailable, and the obvious dangers to human sources must be taken into account: §5.35.

(5) Thus, in sum, no alternative source of intelligence, or combination of alternatives, would be sufficient to substitute for a bulk interception power: §5.41.

20. In the conclusion to Chapter 5 of the Bulk Powers Review, David Anderson QC revisited the conclusion he reached in the Anderson Report concerning the utility of bulk interception (see Observations, §1.35), and stated:

"5.53 This Review has given me the opportunity to revisit my earlier conclusion with the help of Review team members skilled respectively in technology, in complex investigations and in the interrogation of intelligence personnel, and on the basis of considerably more evidence: notably, a variety of well-evidenced case studies, internal documentation and the statistic that almost half of GCHQ's intelligence reporting is based on data obtained under bulk interception warrants.

5.54 My opinion can be summarised as follows:

(a) the bulk interception power has proven itself to be of vital utility across the range of GCHQ's operational areas, including counter-terrorism in the UK and abroad, cyber-defence, child sexual exploitation, organised crime and the support of military operations.

(b) The power has been of value in target discovery but also in target development, the triaging of leads and as a basis for disruptive action. It has played an important part, for example, in the prevention of bomb attacks, the rescue of a hostage and the thwarting of numerous cyber-attacks.

(c) While the principal value of the power lies in the collection of secondary data, the collection and analysis of content have also been of very great utility, particularly in assessing the intentions and plans of targets, sometimes in crucial situations.

(d) The various suggested alternatives, alone or in combination, may be useful in individual cases but fall short of matching the results that can be achieved using the bulk interception capability. They may also be slower, more expensive, more intrusive or riskier to life."

21. Annex 8 to the Bulk Powers Review contains 13 "case studies", illustrating the use of and need for bulk interception, and providing context and a factual underpinning for the conclusions in chapter 5. 4 of those case studies were summarised (albeit in slightly less detail) in the Anderson Report, as to which see Observations, §1.36. The other nine are summarised below. As with the examples in the Anderson Report, their importance speaks for itself:

(1) In 2015, GCHQ used communications data obtained under bulk interception warrants to search for new phones used by individuals known to be plotting terrorist acts in the UK. Following the identification of a new phone number, GCHQ eventually identified an operational cell, and its analysis revealed that the cell had almost completed the final stages of a terrorist attack. The police were able to disrupt the plot in the final hours before the planned attack. Without access to bulk data, GCHQ would not have been able to complete this work at all. See Case Study A8/1.

(2) Following terrorist attacks in France, GCHQ provided support to MI5 and European partners in identifying targets and prioritising leads. GCHQ triaged around 1,600 international leads (in the form of telephone numbers, email addresses or other identifiers) in the days following the attacks. It was necessary quickly to determine whether there was any further attack planning, and to identify leads that should be prioritised for further investigation. Without bulk data, that triage work would have taken much longer – potentially many months – and would have led to GCHQ obtaining an incomplete picture, providing only limited assurance that further attack planning had been identified or ruled out: Case Study A8/3.

(3) During the UK's Afghanistan campaign, analysis of data obtained through bulk interception enabled GCHQ to locate and monitor an armed group that had taken hostages captive. Within 72 hours of the kidnapping, the hostages were located. Analysis of the content of communications obtained through bulk interception indicated that the hostages' lives were in danger. The hostages were successfully rescued. There was no likely alternative method to bulk interception

through which the hostage-takers could have been identified and located, or their intentions revealed: Case Study A8/6.

(4) During the UK's Afghanistan campaign, GCHQ used analysis of data obtained under bulk interception warrants to identify mobile devices in the area of Camp Bastion, the main base for UK forces. Analysis flowing from that data revealed that extensive attacks on Camp Bastion were being planned by multiple insurgents. The information led to several such attacks being disrupted. There was no practical means to obtain the information on a targeted basis. See Case Study A8/7.

(5) GCHQ used bulk interception to identify sophisticated malware placed on a nationally important UK computer network by an overseas-based criminal gang. GCHQ did this by looking for traces of the malware within bulk data. Further analysis of the bulk data identified the infrastructure being used by the criminals to deploy and control the malware. The information obtained by GCHQ eventually led to the arrest of the gang. This is by no means an isolated: GCHQ currently deals with over 200 cyber incidents a month. See Case Study A8/8.

(6) In 2016, a European media company suffered a major, destructive cyber-attack. The analysis of bulk data permitted GCHQ (i) to link this attack to other attacks, and to explain what had happened; and (ii) to identify a possible imminent threat to the UK from the same cyber-attackers. As a result, GCHQ was able to protect government networks, and warn media organisations so that they were able to protect their own networks. GCHQ would have been unable to achieve the same outcome without the use of bulk powers: Case Study A8/9.

(7) Bulk data has given GCHQ significant insight into the nature and scale of online child sexual exploitation activity. In April 2016 alone, GCHQ identified several hundred thousand separate IP addresses worldwide being used to access indecent images of children through the use of bulk data. Further analysis can then lead (for example) to targeting those whose online behaviour suggests they pose the greatest risk of committing physical or sexual assaults against children: see Case Study A8/10.

(8) Between November 2014 and November 2015, GCHQ's analysis of data obtained under bulk interception warrants led to significant disruption of cocaine trafficking, involving the seizure of cocaine with a street value of around £1.1 billion. The traffickers could not have been identified, tracked, and disrupted without the use of bulk interception: Case Study A8/12.

(9) In early 2015, GCHQ's analysis of data obtained under bulk interception warrants was able to identify the multiple communications methods used by the principal members of an organised crime group involved in human trafficking into the UK. The information enabled investigations which eventually resulted in the release of a group of trafficked women, and the individual concerned was subsequently arrested: Case Study A8/13.

Response to Applicants' factual allegations about the s.8(4) regime: §§26-32, 35-47

22. At §§26-30 of the Applicants' Further Observations, the Applicants have sought to define the terms "bulk" and "targeted", such that anything which is "bulk" is effectively indiscriminate and is to be contrasted with a "targeted" capability which is based on "*reasonable suspicion that a specific target*" has committed or is likely to commit a criminal offence or is a threat to national security. But that distinction is unhelpful and unjustified in the present context:

    a. To the extent that it implies that, as part of bulk interception, GCHQ in fact accesses communications about a wide range of people who are of no legitimate interest to the security and intelligence agencies, that is wrong. As made clear by David Anderson QC in the Bulk Powers Review, the s.8(4) regime does not permit interference with communications indiscriminately and only the communications of suspected criminals or national security targets are deliberately selected for examination.

    b. This over-simplistic distinction ignores the incremental collection, filtering and selection process which in fact takes place as set out at §§15-16 above. That careful process incorporates significant safeguards at each stage and

ensures that these activities are necessary and proportionate. Thus, whilst there may be "bulk" collection at the first stage, there is then a sequence of stages applied which ensures that the fragments of intelligence which are actually analysed and pieced together at the end of the process are appropriately targeted at those who in fact pose a threat to the UK i.e. individuals who are of legitimate intelligence interest, regardless of whether they had previously been identified as a threat by the SIAs.

c. Allied to that, it is wrong to suggest that selection other than by reference to a previously identified individual must mean that the interception is untargeted and indiscriminate. Even when there is selection at the third stage on the "complex query" basis i.e. by inputting a number of criteria to narrow down the information which is analysed, that does not mean that communications are available for GCHQ analysts to search through at will. As explained in the Bulk Powers Review, the filtering and complex search process draws out the communications of intelligence value and therefore the odds of a 'false positive' are considerably reduced (see §2.21 of that report at p25). Whilst "complex query" process is closer to true bulk interception (since it involves the collection of unselected content and/or secondary data) it would be wrong to categorise that as indiscriminate since that activity must still satisfy the statutory tests of purpose, together with necessity and proportionality, in order to be lawful. As stated by the Commissioner at §6.5.40 of his 2013 Report[4]:

"What remains after filtering (if anything) will be material which is strongly likely to include individual communications which may properly and lawfully be examined under the section 8(4) process. Examination is then effected by search criteria constructed to comply with the section 8(4) process."

d. In addition, to the extent that it is suggested that activity can only be lawful for Art. 8 ECHR purposes in this context if it is based on "reasonable grounds for suspicion" that is not consistent with the established case law in this area, as discussed in more detail at §§90-97 below.

[4] See Annex 1

23. In terms of the different stages of the bulk interception process, the three stages outlined in the Bulk Powers Review (see §15 above) set this out authoritatively and accurately and are to be preferred, in contrast to the suggested six stages at §31 of the Applicants' further observations. For example, "Initial interception" and "Extraction" are, in fact, one single process i.e. the information is initially obtained by copying it. Stage 4 is a necessary part of any analysis at Stage 3 and therefore both stages are more accurately described under the rubric of "selection for examination" (see §2.17 of the Bulk Powers Review). In addition Stage 6, i.e. any distribution of the results of analysis to other persons or agencies, is outside the scope of the current application and is subject to separate safeguards and controls.

24. Whilst it is right that s.8(4) sets no upper limit on the number of communications that may be intercepted, it does not follow that, even in principle, a single warrant could "*encompass the communications of an entire city in the UK with the residents of another country*" (see Applicants' further observations at §§35-37). That could never be necessary or proportionate (applying the safeguards set out at §§2.69-2.81 of the Observations). It is also fanciful to suggest that this could occur in practice since this could only possibly occur if all such communications were carried on a single telecommunications system and, in practice, there is extraordinary diversity in the supply of communications technologies to consumers.

25. GCHQ does not seek to contend that the limitations on its resources constitute a permissible legal safeguard in this context (contrary to the suggestion at §§38-40 of the Applicants' further observations). As made clear by the ISC it is <u>both</u> for legal reasons and due to resource constraints that GCHQ cannot conduct blanket indiscriminate interception of all communications and most importantly "*it would be unlawful for them to do so, since it would not be necessary and proportionate, as required by RIPA* (see §58 of the ISC Report set out at §1.23 of the Observations).

26. There is also no inconsistency in the Government's description of GCHQ's operations (see §41 of the Applicants' further observations). Whilst it is right that electronic communications do not traverse the internet by routes which can

necessarily be predicted, that does not mean that the first stage of the process (i.e. collection) is or could lawfully be, indiscriminate or wholly untargeted. For example, there may be a very real difference (in terms of necessity and proportionality) between identifying a bearer which carries a high proportion of e-mail traffic flowing out of Syria from one which carries e.g. You Tube videos between states which are unlikely to be of intelligence interest. Accordingly it is an unfair characterisation of the process to suggest that the first stage of the process involves access to "*an enormous amount of data relating to the lives of private individuals around the world, the vast majority of whom are not and never will be of intelligence interest to UK intelligence services*" (see §41 of the Applicants' further observations). That first stage does involve an element of selection and that is just the beginning of a process which narrows down what is actually analysed to that which is strongly likely to include communications of legitimate interest to the SIAs. The Applicants' submissions effectively boil down to a proposition that it could never be Art. 8 ECHR compliant to intercept in bulk prior to selecting for examination. But that is clearly contrary to this Court's approach in *Weber*.

27. In addition and as discussed above, it is wrong to suggest that GCHQ analysts can store and "*trawl*" through a "*large pool of information...by reference to unknown selectors that may bear little or no resemblance to criminal investigations or operations*" (see Applicants' further observations at §42). Whilst it is not understood what is meant by "unknown selectors" in this context (given that GCHQ cannot be expected to make public the selectors it uses), if this is meant to be a description of the "complex query" process at the selection stage (see §2.21 of the Bulk Powers Review), then the characterisation of that process is wholly inaccurate. These searches are designed to draw out communications of intelligence value and other communications which are not of intelligence interest are discarded. That was the clear conclusion of the ISC and Mr Anderson QC (including in the Bulk Powers Review) i.e. oversight bodies who have direct experience of the process in practice.

28. It follows that the example which is given at §§44-46 of the Applicants' further observations, namely that bulk interception could result in "*everyone's reading activities*" being "*automatically intercepted, stored and made available for analysis*" is

utterly far-fetched. Whilst, in principle, a selector could be used to identify everyone who had downloaded a particular book or article from the internet, there are safeguards in place which ensure that any selector is justified on necessity and proportionality grounds and technical measures are also in place (by way of a triage process) to ensure that a selector which produces too many items for examination is refined before the results can be looked at by an analyst. The sophistication of the selection process ensures that the system is more proportionate, not more intrusive, contrary to the impression given in the Applicants' submissions.

29. It is also misleading to suggest that "*the dragnet of bulk intercept includes routine and automated storage and analysis of the communications of human rights activists*" (§47 of the Applicants' further observations). That could never be necessary or proportionate and was contrary to the express findings of the IPT in its Third Judgment (dated 22 June 2015) in which it made clear that GCHQ had lawfully and proportionately intercepted and selected for examination communications of the two Applicants (as explained in detail at §§4.102-4.103 of the Observations).

Is the Government constrained by NCND in this context? (§§48-52)

30. At §§48-52 of the Applicants' further observations it is said that the Government is not constrained from responding more fully to the factual allegations which have been made about its bulk interception activities and is seeking to hide behind a "self-imposed" policy of Neither Confirm Nor Deny (NCND). It is also suggested that the NCND principle has been called into question by the domestic courts.

31. This ignores the fact that the NCND principle was accepted in *Kennedy v United Kingdom*[5] as a valid basis on which information could be withheld (see §187) and was also recognised in *Klass* at §58, *Weber* at §135 and *Segerstedt-Wiberg v Sweden*, judgment 6 June 2006 at §102. It remains an important mechanism through which the state discharges its positive obligations (including under Arts. 2 and 3 ECHR) to protect information which, if disclosed, would be harmful to the public interest. Most recently in the domestic setting the principle was reviewed by Lord Justice

[5] App. 26839/05, 18 May 2010

Pitchford in the context of the 'Undercover Policing Inquiry'[6] who considered evidence from a Senior Cabinet Office National Security Adviser. There was no suggestion in that careful review of the application of the principle that it was unimportant or capriciously applied (see, in particular, §§116, 127, 145-146 of that Ruling).

'New' facts: §§53-55

32. In terms of the 'new facts' referred to at §§53-55 of the Applicants' further observations (and addressed at §§4-9 of the Applicants' Factual Appendix) these are neither confirmed nor denied. As discussed above, it has been a principle of successive UK Governments neither to confirm nor deny ("NCND") assertions, allegations or speculations in relation to the Intelligence Services, whose work requires secrecy if it is to be effective.

33. In any event, as appears to be acknowledged by the Applicants at §55 of their further observations, these allegations are irrelevant to the issues which have been raised in these applications.

Intrusiveness of interception content and communications data: §§56

34. As explained at §§4.29-4.31 of the Observations, the Court has correctly recognised in *Malone v UK* (app. 8691/79, Series A no.82) that it is less intrusive in Article 8 terms to obtain communications data than the content of those communications. That remains the same even in relation to internet-based communications. The aggregation of communications data may in certain circumstances (and potentially, with the addition of further information that is not communications data) yield information that is more sensitive and private than the information contained in any given individual item. However, it remains the case that, if like is compared with like, the interception of communications raises greater privacy concerns. For example, the content of 50 communications is very likely to be more intrusive in

[6]Annex 2. Restriction Orders: Legal Principles and Approach Ruling 3 May 2016:

Article 8 terms than the communications data associated with those 50 communications.

The Intelligence Sharing Regime: §§33-34, 62-77, 226-231

35. In their further observations the Applicants make wide-ranging submissions about the nature of US surveillance law. It is unnecessary and inappropriate for the Court to make findings about that law in this Application.

36. The Applicants' further observations also address alleged US surveillance activities outside the scope of this Application. The Application is about the UK's alleged receipt of information from the USA's Prism and Upstream programmes[7], which the NSA operates under the authority of s.702 FISA. The Applicants address the NSA's surveillance activities under a completely different authority (Executive Order, "EO" 12333) (see §§64-68 and §77 of the Applicants' further observations and see §§10-12 of the Applicants' Factual Appendix). It is unnecessary and inappropriate to address EO 12333.

37. In those circumstances, the Government makes the following key points in response to these aspects of the Applicants' further observations.

38. **First** insofar as the intelligence activities and operations of the US Government have been the subject of official statements and/or other express avowal by the executive branch of the US Government, the Government does not adopt the NCND principle in relation to them. But some caution should be exercised when considering allegations which have not been publicly avowed by the US Government. In that regard the Government wishes to draw to the Court's attention the Executive Summary of the Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden, published by the U.S. House of Representatives on 15 September 2016[8]. In this document the House Permanent

[7] See e.g. Applicants' Additional Submissions on the Facts and Complaints at §§5-8.

[8] Annex 3. Executive Summary of the Review of the Unauthorised Disclosures of Edward Snowden published on 15th September 2016

Select Committee on Intelligence finds that "*the public narrative popularized by Snowden and is allies is rife with falsehoods, exaggerations, and crucial omissions*" (p1). They also find that it is "*not clear Snowden understood the numerous privacy protections that govern the activities of the [U.S. Intelligence Community]. He failed basic annual training for NSA employees on Section 702 of the Foreign Intelligence Surveillance Act (FISA) and complained the training was rigged to be overly difficult. This training included explanations of the privacy protections related to the PRISM program that Snowden would later disclose*" (p3). The Committee concluded that Snowden "*was, and remains, a serial exaggerator and fabricator. A close review of Snowden's official employment records and submissions reveals a pattern of intentional lying*" (p3).

39. **Secondly** it is incorrect to suggest that Presidential Policy Directive 28 ('PPD-28') places no restrictions on the collection of signals intelligence in bulk (see §64 of the Applicants' further observations). PPD-28 requires that "[*s]ignals intelligence activities shall be as tailored as feasible*" and, as noted in the Letter from Robert Litt, General Counsel of the Office of the Director of National Intelligence dated 22 February 2016 ('the Litt Letter')[9] "*[t]his means, among other things, that, whenever practicable, signals intelligence collection activities are conducted in a targeted manner rather than in bulk*".

40. **Thirdly** it is wrong to characterise Upstream and Prism as "bulk" programmes, in direct contrast to programmes which are "targeted" (see §71 of the Applicants' further observations and §§13-19 of their Factual Appendix). As made clear by David Anderson QC in the Bulk Powers Review, although the powers under FISA s.702 do concern "bulk interception" the powers are focused and targeted and bear a strong resemblance to GCHQ's 'strong selector' process. That was made clear at §§3.56-3.65 of that Report, including in the following passages:

"***There are marked similarities between the s702 programme and bulk interception as practised in the UK, particularly via the "strong selector process"*** *summarised at 2.19(a) above:*

(a) Both are ***foreign-focused capabilities****, based on the interception of a cable and the collection of "wanted" communications* ***by the application of strong selectors.***

[9] at 4-6 (Annex VI to the Privacy Shield documents) (http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-6_en.pdf).

(b) The application of those selectors from a very early stage ***gives both the flavour of targeted capabilities****, though as explained at 2.19(a) above, the holding of communications in bulk for a short period means that a bulk warrant will be required under the Bill.*

(c) Both offer the advantages of operational scale and flexibility to service the range of foreign intelligence missions.

(d) Even the authorisation regimes are similar, with external authorisation of the intelligence purposes for which the data can be accessed and used and the procedures for targeting and handling of information, but with decisions relating to individual selectors being delegated to GCHQ / NSA.

...

The s702 arrangements continue to permit the ***targeted selection*** *and retention by the NSA of wanted communications from bulk internet traffic, in very much the same way as the strong selector process described at 2.19(a) above.* (emphasis added)

41. In those circumstances, the Applicants are wrong to assert that David Anderson QC "endorsed" Upstream as a non-targeted capability in the Bulk Powers Review.

42. Collection under s.702 of FISA is based on specific and identified targets and it may not be carried out on an indiscriminate basis. It must comply with the Fourth Amendment to the US Constitution, statutory restrictions contained in s.702 itself, and Court-approved targeting procedures.

43. The activities under s. 702 must be targeted at specific selectors such as e-mail addresses or phone numbers. The Privacy and Civil Liberties Oversight Board (PCLOB) found that the US government must make targeting "*determinations (regarding location, U.S. person status, and foreign intelligence value) about the users of each selector on an individualized basis[;] it cannot simply assert that it is targeting a particular [ ] group*."[10] The PCLOB's report led to the European Commission's finding, in its adequacy decision assessing the EU-U.S. Privacy Shield Agreement, that acquisition pursuant to s. 702 is "*carried out in a targeted manner through the use of individual selectors that identify specific communications facilities, like the target's e-mail address or telephone number, but not key words or even the names of targeted individuals*."[11]

[10] PCLOB Report at 21.
[11] *See* Adequacy Decision at para. 81 (p. 22), *available at* http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf.

44. Collection activities under s. 702 are also limited to specific and defined intelligence priorities set by policy-makers.[12] These priorities include topics such as nuclear proliferation, counterterrorism, and counter-espionage.

45. "Upstream collection" involves the acquisition of communications as they transit the telecommunications "backbone" networks (including the Internet "backbone") of US telecommunications-service providers.[13] Tasked selectors are sent to providers operating these networks after the government applies its targeting procedures to each individual selector.[14] Upon receipt of the tasked selectors, the service providers must assist the Government in acquiring communications to, from, or otherwise containing these selectors while they transit the 'backbone.'[15] Communications are filtered for the purpose of eliminating wholly domestic communications, and then scanned to capture communications containing tasked selectors.[16] Communications that successfully pass both these filtering screens are then ingested into NSA databases.[17]

46. Before communications facilities may be targeted for intelligence collection, a written certification must be submitted to and approved by the FISA Court[18] which must include targeting procedures.[19] The targeting procedures ensure that collection takes place only as authorised by statute and within the scope of the certifications. Under these limitations, as the PCLOB concluded, collection "*consists entirely of targeting specific persons about whom an individualized determination has been made*."[20]

47. Collection is targeted through the use of individual selectors, such as email addresses or telephone numbers. To target these selectors, US intelligence personnel must

---

[12] *See* Letter from Robert Litt, General Counsel of the Office of the Director of National Intelligence, dated Feb. 22, 2016, at 4-6 (Annex VI to the Privacy Shield documents) (http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-6_en.pdf) (Litt Letter), discussed below.
[13] *See* PCLOB Report at 35; PRG Report at 141 n.137.
[14] See PCLOB Report at 36.
[15] PCLOB Report at 35–37. *See also* Litt Letter.
[16] PCLOB Report at 37.
[17] *Ibid*.
[18] 50 U.S.C. §1881a (a) and (b) – the FISA Court is a US federal court established and authorized under the Foreign Intelligence Surveillance Act of 1978 (FISA).
[19] *See* 50 U.S.C. § 1881a (d).
[20] *See* PCLOB Report at 103.

determine, pursuant to targeting procedures approved by the FISA Court, that they are likely being used to communicate foreign intelligence information that falls within the categories covered by the certification submitted to the court.[21] The reasons for selecting a target must be documented[22].

48. The Department of Justice and ODNI (Office of the Director of National Intelligence) review the documentation for every selector to assess compliance with the requirements of the targeting procedures – i.e. that all three requirements are met: that the user is reasonably believed to be (i) a non-US person, (ii) located outside the US, and (iii) who there is a valid foreign intelligence reason for targeting.[23]

49. As part of its review of the certification, the FISA Court must assess the targeting and minimization procedures against the reasonableness requirements of the Fourth Amendment. While the targeting and minimization procedures are primarily concerned with the privacy of US persons, the targeting procedures require that before a non-US person's selector is targeted for s.702 acquisition, the US government must include a written explanation for each individual tasking decision. This tasking decision contains the basis for the government's determination that collection on the particular target will likely return foreign intelligence information relevant to the subject of one of the certifications approved by the FISA Court.[24]

50. Thus, the targeting procedures protect the privacy of non-US persons by ensuring that each individual targeting decision is based upon a sufficient nexus to the foreign intelligence information sought to be obtained by one of the FISC-approved certifications. Similarly, the written certification approved by the FISA Court must include minimization procedures. The minimization procedures for s.702 have been

[21] 50 U.S.C. §1801(e). For example, the US might target the user of a specific email address or telephone number based on credible information indicating that the email address or telephone number (a "selector") is believed to be used by a foreign terrorist operating overseas.
[22] For example, the government would specify how it was able to reasonably assess that the selector is used by a foreigner located outside the US and what foreign intelligence information (e.g., terrorism) the government expects to obtain from targeting the user of the selector.
[23] 50 U.S.C. §1881a(l); *see also* NSA Director of Civil Liberties and Privacy Report, *NSA's Implementation of Foreign Intelligence Surveillance Act Section 702* (hereinafter "NSA Report") at 4, available at http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.
[24] *See* PCLOB Recommendations Assessment Report, February 5, 2016, at 14-15.

publicly released.[25] These procedures focus on US persons but also provide important protections to non-US persons.

51. The US Intelligence Community must also comply with the privacy protections afforded to non-US persons by Presidential Policy Directive 28 (PPD-28) – see §§1.13-1.14 of the Observations (and see also the Litt Letter). This extends certain protections afforded to the personal information of US persons to non-US person information (and see further §141 below)[26].

52. In those circumstances, the programmes which are carried out under the authority of s.702 of FISA can properly be described as "targeted" and certainly do not involve the indiscriminate bulk collection of data.

53. **Finally**, in §69 of their further observations, the Applicants refer to media reports which describe Prism (collection under s.702 of FISA) as a programme under which the US was "*tapping directly into central servers*". However, as the Applicants concede in the Factual Appendix (see §19), that statement is inaccurate. An accurate description of how the programme operates can be found in the PCLOB Report dated July 2014 (see the Observations at §1.8).

LEGAL FRAMEWORK

The Applicants' summary of the legal framework §§82-126

54. The Government has set out in detail the legal framework which applies to the Intelligence Sharing and s.8(4) regimes at pp59-103 of the Observations. In terms of the Applicants' further observations on the current legal framework, the Government makes the following key submissions in response.

[25] The minimization procedures are available at http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf; http://www.dni.gov/files/documents/ppd-28/2014%20FBI%20702%20Minimization%20Procedures.pdf; and http://www.dni.gov/files/documents/ppd-28/2014%20CIA%20702%20Minimization%20Procedures.pdf.

[26] NSA's unclassified and publicly available PPD-28 procedures apply to all of NSA's signals intelligence activities, including activities undertaken under s.702 - *see, e.g.*, NSA PPD-28 Implementation Procedures, Section 7.2.

55. As regards the intelligence sharing regime:

    a. It is inaccurate to say (at §89 of the Applicants' further submissions), that when the Applicants initiated proceedings in the IPT there was "*no information in the public domain setting out the rules governing intelligence sharing between the UK Government and foreign intelligence agencies*". As set out at §§2.1-2.22 of the Observations that regime was set out in primary legislation.

    b. In terms of the Disclosure which was recorded in the IPT's 5 December and 6 February Judgments (see §93 of the Applicants' further observations), since it formed part of a judicial decision it can be taken into account in assessing "forseeability" for Art. 8(2) ECHR purposes – see the Observations at §2.23 and footnote 63. Therefore, prior to being incorporated into the Code, the domestic position was the same as a result of the 5 December 2014 and 6 February 2015 IPT judgments.

56. In terms of the oversight provided by the Investigatory Powers Tribunal (see §§96-100 of the Applicants' further observations):

    a. The IPT decision in *Human Rights Watch v Secretary of State for the Foreign and Commonwealth Office et al* [2016] UKIP Trib 15/165/CH, 16 May 2016, was a response to a worldwide campaign by Privacy International which encouraged individuals to bring claims in the IPT in order to find out "*if GCHQ illegally spied on you*". When addressing whether a sample of claimants had victim status to bring ECHR claims, the IPT applied the recent guidance in *Zakharov v Russia*, 4 December 2015, Application No. 47143/06[27]. That was

[27] The IPT concluded: "*We are satisfied that the appropriate test for us to operate, which would accord with Zakharov and our obligations under RIPA, is whether in respect of the asserted belief that any conduct falling within subsection s.68(5) of RIPA has been carried out by or on behalf of any of the Intelligence Services, there is any basis for such belief; such that the "individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or legislation permitting secret measures only if he is able to show that due to his personal situation, he is potentially at risk of being subjected to such measures." (Zakharov at 171). This continues to be the low hurdle for a claimant that this Tribunal has traditionally operated*."

not an "abandoning" of the approach noted by this Court in *Kennedy*[28]; it was a legitimate application of the victim test at §171 of *Zakharov*. As the IPT itself noted in the final sentence of §46 of its judgment "*This continues to be the low hurdle for a claimant that this Tribunal has traditionally operated.*"

b. There is nothing improper, as a matter of principle, in the IPT receiving briefings from the SIAs as part of their work. The IPT is a specialist tribunal and the nature of its casework means that it is necessary for its members to have a level of background understanding regarding the agencies' practices and procedures. The meeting which occurred at Thames House on 28 September 2007 (as recorded in a Note for File dated 15 November 2007) was an entirely appropriate example of that and the suggestion that it somehow undermines the independence or effectiveness of the IPT is strongly resisted.

c. As is clear from a proper reading of the Note for File which recorded that meeting:

   i. The purpose of the visit was a "general briefing", including about MI5's data handling techniques and the growth and changes to MI5 and the scale of the threat that it was facing.

   ii. As part of the data handling presentation MI5 indicated that, for the purposes of IPT proceedings, it would not routinely conduct searches of "reference data-bases" i.e. databases containing information about the population generally (e.g. the Voter's Roll or telephone directories), for any mention of a complainant's name and such searches would only be carried out if the data was "*relevant or had been relied on in the course of an investigation*" (see Annex C to the Note for File).

   iii. That was an entirely sensible and proportionate suggestion, since the fact that a complainant's name was on e.g. a Voter roll which had

[28] See the Applicants' further observations at §97.

never been accessed by officers at MI5 could not conceivably be relevant to whether there had been unlawful conduct in relation to an individual.

iv. As made clear from the Note for File the meeting was an opportunity for MI5 to make clear what its standard position would be. It would be open to the IPT on a case by case basis and in response to any particular complaint to decide that such an approach should not be followed and to require more extensive searches as necessary[29].

> Indeed, that has very recently occurred in domestic proceedings in the IPT concerning the lawfulness of bulk personal datasets, where the IPT has ordered the Respondents to carry out searches of their databases (including their Bulk Personal Datasets and Bulk Communications Datasets)"[30]

d. In addition, it cannot sensibly be suggested that this meeting in any way undermines the independence or effectiveness of the IPT's examination of the s.8(4) or intelligence sharing regimes:

i. The complaints were not about the holding of bulk personal datasets i.e. "reference data-bases" which have been the subject of separate and more recent proceedings in the IPT[31]. They were about interception under the s.8(4) RIPA regime and intelligence sharing with the US. (Similarly, in these proceedings, there is no complaint about the use of bulk personal datasets, which are the subject of an entirely different legal regime and therefore wholly outwith the scope of the application.)

---

[29] That is consistent with the standard form of words which MI5 uses when responding to an IPT complaint which makes clear the position it has adopted as regards searches of reference data. That standard form of words is as follows: *""When checking our records in response to complaints to the IPT, we would not normally search reference databases containing information about the general population, eg the electoral roll, telephone directories etc, for a trace of the complainant's name. We would only do so if it appeared relevant to the complaint and/or the Tribunal specifically requested it. This was discussed and agreed with Tribunal members when they visited Thames House on 28 September 2007. In this case, we have not checked reference databases for any mention of Mr [name redacted]. If the Tribunal requires us to do so, please let us know*."

[30] IPT Bulk Data Directions Searches Order 12 December (Annex 8 attached)

[31] Annex 4. See the recent judgment of the IPT in *Privacy International v Secretary of State for Foreign and Commonwealth Affairs & Others* [2016] UKIPTrib 15_110-CH

ii. The meeting occurred six years before the Applicants brought claims in the IPT and only one of those who attended the meeting was part of the panel of five who heard the complaints.

iii. The Applicants' suggestion that reference data such as the Voter's roll or telephone directories should have been searched as part of their complaint about "bulk interception" is therefore not understood.

iv. The searches which were conducted in the IPT proceedings were plainly adequate, not least because unlawful conduct was identified in respect of two of the complainants.

v. The IPT was assisted throughout the proceedings by Counsel to the Tribunal (CTT) who was able to make submissions (as appropriate) on the adequacy of the search process by GCHQ and the other respondents (GCHQ being the primary respondent given the nature of the allegations in the proceedings).

57. In addition, the Applicants' criticisms of the ISC and the Commissioner are misplaced (see §§101-107 of the Applicants' further observations). Whatever the position historically, it cannot be said that the ISC has devoted little attention to scrutinising the Government's interception programmes, as is evident from its detailed report in March 2015 discussed at e.g. §§1.3, 1.19, 1.21, 1.23-1.24, 1.26, 1.33 of the Observations.

58. As to the suggestion that the part-time status of the Commissioner means that he is unable to provide effective oversight, that has not been suggested by the Commissioner himself. In his 2013 Annual Report he stated that his investigations are "*thorough and penetrating*" and that he has "*no hesitation in challenging the public*

authorities wherever this has been necessary" (at §6.3.3[32]). That sentiment was also reiterated e.g. in his 2015 Annual Report[33].

59. At §§108-115 and §137 of the Applicants' further observations it is said that certain proposed changes to the UK domestic legal framework for investigatory powers, as set out in the Investigatory Powers Bill 2016 (which received Royal Assent on 29 November 2016 as the Investigatory Powers Act, though most of the Act is not yet in force), demonstrate that the current legal framework is "unfit for purpose" and that the Government's position in these proceedings is "unsustainable". But it is important to recognise that the Investigatory Powers Act deals with a wide range of powers, the vast majority of which are beyond the scope of this application. The intention of the Act is to provide an up to date framework for the use (by the SIAs, law enforcement and other public authorities) of investigatory powers to obtain communications and communications data[34]. It addresses not just the interception of communications, but also the retention and acquisition of communications data and equipment interference activity. It will essentially consolidate and build upon the range of current statutory powers in these areas.

60. That a need has been identified for the updating and consolidating of existing legislation, cannot lead to the conclusion that the s.8(4) regime or the intelligence sharing regime is unlawful. That was not the conclusion of the IPT, having investigated these matters in considerable detail. Nor was that any part of the Joint Committee's Report on the Draft Investigatory Powers Bill (see §113 of the Applicants' submissions), whose remit was not to opine on the compatibility of those two regimes with the ECHR[35].

[32] Annex 1. ***Commissioner's Annual Report 2013***

[33] Annex 5. Commissioner's Annual Report 2015. At 2.2 he stated: "*The Commissioner is independent of Government and Parliament and must report half-yearly7 to the Prime Minister on the carrying out of his functions. Independent oversight plays a key role in contributing to accountability. The purpose of oversight is to ensure that there are strong checks and balances, demanding and visible safeguards, and that public authorities are held to account*."

[34] See the Explanatory Notes to the Bill at Annex 7.

[35] See the Joint Committee on the Draft Investigatory Powers Bill, Report, HL Paper 93-HC 651 at Annex No. 26 of the Applicants' Reply. The role of the Joint Committee was to conduct pre-legislative scrutiny of the draft Bill and to make recommendations about the Bill.

Applicants' summary of the procedural history: §§116-126

61. The Government has set out the procedural history to these Applications at pp53-59 of the Observations. In particular it is to be noted that the Applicants are wrong to suggest that they were not represented at the closed hearing on 10 September 2014 at which time the IPT considered the sensitive arrangements governing the s.8(4) and intelligence sharing regimes. As explained at §§7.32-7.35 of the Observations Counsel to the Tribunal (CTT) was appointed in the domestic IPT proceedings and, in practice in this case, performed an essentially similar function to that of a special advocate (see §10 of the 5 December judgment). In those circumstances it is misleading to state that there was no one representing the interests of the applicants in the closed hearing.

LEGAL SUBMISSIONS

Intercepting communications data is as intrusive as intercepting content: §§-134

62. The general answer to this assertion is set out at §§4.29-4.33 and 4.57-4.64 of the Observations i.e. in summary:

(1) The Court has correctly recognised in *Malone v UK* (app. 8691/79, Series A no.82) that it is less intrusive in Article 8 terms to obtain communications data than the content of those communications (see §34 above).

(2) As a result, the Court has rightly not applied the *Weber* safeguards to the acquisition of communications data (as opposed to content).

(3) Similarly, the Court has not applied the *Weber* safeguards to other forms of surveillance (e.g. the installation of GPS in a suspect's car – see *Uzun v Germany* app. 35623/05): which is a strong indicator that the *Weber* criteria should not apply to the acquisition of related communications data under the s.8(4) Regime.

(4) Therefore, the test should be the general one whether the law indicates the scope and manner of any discretion with sufficient clarity to give the individual

adequate protection against arbitrary interference. The s.8(4) Regime satisfies that test as regards communications data, for all the reasons in §§4.57-4.64 of the Observations.

(5) In any event, it should be noted that the s.8(4) Regime distinguishes between communications content, and "related communications data". "Related communications data" has a specific statutory meaning which is not synonymous with "metadata", or "behavioural data. Much "metadata" or "behavioural data" is content for the purposes of the s.8(4) Regime, and is thus subject to the controls for content. For example, information about the internet pages that a user visits on a particular site would be content, not RCD for the purposes of the s.8(4) Regime.

(6) Further, if the *Weber* safeguards did apply to "related communications data", those safeguards would on a proper analysis be met by the s.8(4) Regime.

63. As explained at §§4.17-4.27 of the Observations, *Digital Rights Ireland* is not relevant to the current application, not least because that case did not concern a national regime or any provision governing access to, or use of, retained data by national law enforcement authorities. Nor does the quotation from §27 of the judgment (see §130 of the Applicants' further observations) address the comparative level or intrusiveness as between content and communications data.

64. Further the Advocate General in *Tele2 Sverige* & *Watson*[36] was addressing (in Part 6 of his opinion) the proportionality of "*general data retention obligations*" (§250) including "*the retention of data relating to all communications effected within the national territory procure in the fight against serious crime*" (§251). It was in that specific context that he referred to the risks associated with access to such data being great or even greater than those arising from access to the content of communications (§§257-259). And he specifically contrasted "*targeted surveillance measures*" when reaching these conclusions which he considered were different from "*general data retention obligations*" (§256). For the avoidance of doubt, the Government reserves the right to

[36] Joined Cases C-203/15

make further submissions on the relevance of these proceedings once judgment has been handed down by the CJEU.

65. Similarly it is not correct to equate any powers to obtain related communications data under the s.8(4) regime with the US's telephony collection programme under s.215 of the USA Patriot Act ("the s.215 Power") (see §§133 of the Applicants' further observations).

    a. First it is to be noted that PCLOB found not only that the s.215 Power raised serious constitutional concerns, but also that it had *"shown minimal value in safeguarding the nation from terrorism"*. In part as a result of PCLOB's findings, the s.215 Power was allowed to lapse by the USA, and was replaced by a different programme under the USA Freedom Act which addressed the issues raised by PCLOB.

    b. Secondly, the collection of telephony metadata pursuant to the s.215 Power is not remotely equivalent to powers exercised pursuant to the s.8(4) Regime. The s.215 Power did not concern interception at all. It authorised the bulk acquisition of telephone records generated by certain telephone companies in the United States, and their storage in a single database. That is not what the s.8(4) Regime authorises, or does. Rather, the closer analogue to the s.8(4) Regime is the USA's surveillance programme under s.702 FISA: a power that PCLOB found to be both constitutional and of high and increasing value. See generally the Bulk Powers Review at §§3.50-3.65 and §§40-52 above.

Forseeability and accessibility: §§135-138

66. To the extent that it is sought to be suggested that *Zakharov* introduces any new (and heightened) test of forseeability in this context, that is not accepted. In this context, the essential test remains whether the law indicates the scope of any discretion, and the manner of its exercise, with sufficient clarity to give the individual adequate protection against arbitrary interference: see §68 of *Malone v UK*. The Grand

Chamber confirmed in *Zakharov* that this test remains the guiding principle when determining the foreseeability of intelligence-gathering powers (see §230).

Internal versus external communications: §§139-

67. This has been addressed in detail at §§4.66-4.76 of the Observations. In addition:

a. It was very well understood at the time RIPA was passed that the s.8(4) Regime would necessarily entail the interception of all communications flowing down a bearer or bearers; and that this would mean intercepting both "internal" and "external" communications. Precisely those points were made in Parliament by Lord Bassam of Brighton when the Bill which became RIPA was debated: see Observations, §1.37. Moreover, RIPA itself provides for, and authorises, the necessary interception of internal communications in the course of the execution of a s.8(4) warrant for the interception of external communications: see s.5(6) RIPA.

b. The description in Mr Farr's witness statement of how the definition of "external communications" in s.20 RIPA applies to particular forms of internet-based communication is no more than the application of a clear definition to certain common and current forms of internet usage. In any event, and as already explained in the Observations, the question precisely how the definition of "external communication" applies to particular forms of internet usage is substantially irrelevant to the operation of the s.8(4) Regime. See Observations, §§4.71-4.76.

c. Contrary to what is asserted at §§141-142 of the Applicants' further observations, the distinction which Mr Farr draws between communications which are received inside and outside the UK is entirely consistent with what was said to Parliament (and what is set out in the Code). If e.g. a communication is received by a platform in the US and is intended to be seen by a wide audience then it is logical that it would be classified as 'external' (see Mr Farr at §§134-138). Moreover, Mr Farr also makes the point (see §137

of his statement) that if e.g. an e-mail is being sent to a specific individual, then the question whether or not the communication was internal or external would depend upon where that individual was located and not on how the e-mail was routed. Consequently there is nothing in Mr Farr's evidence which contradicts the assurances given to Parliament when RIPA was debated.

d. The Government has accepted that the nature of electronic communications over the internet means (and has always meant) that the *factual* analysis of whether a particular communication is internal or external may, in individual cases, be a difficult one (see §4.70 of the Observations). But any such difficulties in how the distinction applies to any *particular* communication is irrelevant in circumstances where it is in practice inevitable (and entirely foreseeable) that, when intercepting material at the level of communications links, both internal and external communications will be intercepted (see §4.71 of the Observations).

e. Importantly the safeguards at the selection for examination stage for communications intercepted under a s.8(4) warrant do not make any distinction between internal or external communications: the safeguards apply equally to both. That means that the s.16 safeguards are not somehow "lost" for UK-based persons if their communications are categorised as external communications (see §§4.73-4.76 of the Observations)[37].

f. Any complexities which may arise in practice in terms of the definition of external and internal communications, do not demonstrate an "apparent indifference" towards the importance of ensuring that there is a clear and accessible regime for bulk interception (as asserted at §§146-147 of the Applicants' further observations). It is a recognition that the way in which

[37] For example, in the case of a Google search, or a YouTube viewing, if the searcher or viewer were in the British Islands, GCHQ could only have selectors that were referable to them as they would be the only individual in relation to whom communications with Google and YouTube could be selected, and such selection would accordingly be done in accordance with the requirements of s.16 RIPA. Whether the communication to be selected were in fact external or internal would be irrelevant. Their interception under the applicable s.8(4) warrant would be lawful (whether by virtue of s.8(4) or s.5(6)(a)), but GCHQ could not examine them if the Secretary of State had not certified that their examination was necessary by means of a modification to the certificate accompanying the s.8(4) warrant (see §4.75 of the Observations).

modern communications systems work will, in practice, inevitably lead to difficult decisions as to how particular communications can be categorised under any legal system. It also involves a proper focus on the essential test for forseeability, namely whether the law indicates the scope of any discretion, and the manner of its exercise, with sufficient clarity to give the individual adequate protection against arbitrary interference: see §68 of *Malone v UK* and §230 of *Zakharov*. The safeguards which apply regardless of whether the communication is internal or external are central to that.

The framework for analysing the claims: §§148-156

68. The Applicants assert that there is a material difference between the strategic monitoring considered in *Weber* and the s.8(4) regime (see §§148-150). They also assert that the "minimum safeguards" in *Weber* are no longer sufficient to address modern forms of communication surveillance (§§152-156 of the Applicants' further observations).

69. Neither proposition is correct. First there are close parallels with the regime which was considered in *Weber,* as explained in detail at §§4.11-4.12 of the Observations. To assert, as the Applicants do, that the persons liable to be affected by s.8(4) are "*every person who uses the internet*" is a gross and inaccurate exaggeration for the reasons explained in detail at §§5-29 above. It is also important to recognise that the test is not whether, in one or more respects, the s. 8(4) Regime is somehow broader or less tightly defined than the German strategic monitoring regime at issue in *Weber*, not least because the strategic monitoring in that case satisfied the "in accordance with the law" requirement by some margin, in that the Art. 8 complaint in *Weber* was thrown out as "manifestly ill-founded": §138.

70. Secondly to the extent that it is suggested that the decision of the Fourth Section in *Szabo* suggests that the minimum safeguards in *Weber* need to be enhanced in this particular context, that is not accepted.

71. The observations made in *Szabo* were made in the context of a regime which, it was found, allowed ordering of interception entirely by the Executive, with no assessment of strict necessity, with potential interception of individuals outside the operational range and in the absence of any effective remedial or judicial measures (see §17 and §52). Those cumulative factors led the Court to find a violation of Article 8 ECHR. Crucially (and pertinent to the distinction between mass interception and mass surveillance) the Court found there to be no or no adequate controls preventing the examination of communications following interception.

72. In the judgment the Court expressly acknowledged that bulk interception was proportionate in order to meet modern security threats, but that the issue was whether the applicable safeguards were adequate, at §68:

> "[I]*t is a natural consequence of the forms taken by present-day terrorism that governments resort to cutting-edge technologies in pre-empting such attacks, including the massive monitoring of communications susceptible to containing indications of impending incidents* […] *In the face of this progress the Court must scrutinise the question as to whether the development of surveillance methods resulting in masses of data collected has been accompanied by a simultaneous development of legal safeguards securing respect for citizens' Convention rights*".

73. Insofar as the Court identified a need to enhance Convention case-law on interception (§70), this was for the purpose of addressing surveillance practices, specifically involving the acquisition and retention of detailed profiles of intimate aspects of citizens' lives. As addressed in detail at the outset of these further Observations (and at §§1.21-1.25 of the main Observations), the s.8(4) regime is not one of "mass surveillance".

Alleged absence of mandatory minimum safeguards: §§157-183

(1) The nature of the "offences" which may give rise to an interception order

74. At §§159-160 of the Applicants' further observations it is suggested that bulk interception cannot be lawful in the absence of suspicion that a particular offence has been or may have been committed.

75. This is not what the law requires. It is not mandated by Article 8 ECHR, and it would in practice denude the interception of communications under the s.8(4) Regime of a very large portion of its utility, thereby endangering the lives of UK citizens.

76. Much of the aim of interception pursuant to the s.8(4) Regime is not to search for the communications of identified targets. Rather, it is to ascertain, via the application of complex searches, who should be a target in the first place ("target discovery"). It is to identify who are the individuals, groups and organisations outside the UK that pose a threat to the UK, because without such a power the Intelligence Services would be unable to tell who they were. See for example the Bulk Powers Review at §5.3:

"Bulk interception is a capability designed to obtain foreign-focused intelligence and identify individuals, groups and organisations overseas that pose a threat to the UK. It allows the security and intelligence agencies to intercept the communications of individuals outside the UK and then filter and analyse that material in order to identify communications of intelligence value.

Bulk interception is essential because the security and intelligence agencies frequently have only small fragments of intelligence or early, unformed, leads about people overseas who pose a threat to the UK. Equally, terrorists, criminals and hostile foreign intelligence services are increasingly sophisticated at evading detection by traditional means. Just as importantly, due to the nature of the global internet, the route a particular communication will travel is hugely unpredictable. Combined, this means that sometimes the data acquired via bulk interception is the only way the security and intelligence agencies can gain insight into particular areas and threats…"

(Emphasis added)

77. See too Annex 7 to the Bulk Powers Review, which sets out GCHQ's "Statement of Utility of Bulk Capabilities", supplied to the Review in July 2016, stating inter alia:

"GCHQ would not be able to identify those who wish us harm without bulk powers. Terrorists, child abusers, drug traffickers, weapons smugglers and other serious criminals choose to hide in the darkest places on the internet. GCHQ uses its bulk powers to access the internet at scale so as then to dissect it with surgical precision.
By drawing out fragments of intelligence from each of the bulk powers and fitting them together like a jigsaw, GCHQ is able to find new threats to the UK and our way of life; to track those who seek to do us harm, and to help disrupt them.

- ***Bulk Interception:*** *Interception provides valuable information that allows us to discover new threats. It also provides unique intelligence about the plans and intentions of current targets – through interception of the content of their communications. Communications data obtained through bulk interception is also*

> *crucial to GCHQ's ability to protect the UK against cyber-attack from our most savvy adversaries and to track them down in the vast morass of the internet."*

(Emphasis added)

78. See also the ISC's Report[38] at vii on page 3 ("Key Findings"), under the heading "Why do the Agencies intercept communications?"

> *"(b) As a "discovery" or "intelligence-gathering", tool. The Agencies can use targeted interception only after they have discovered that a threat exists. They require separate capabilities to uncover those threats in the first place, so that they can generate leads and obtain the information they need to then target those individuals…"*

79. Turning to the various examples of the use of bulk interception powers under the s.8(4) Regime given in Appendix 8 to the Bulk Powers Review, and set out at §22 above, well over half of the examples concern the discovery of previously unknown targets through the use of a bulk interception capability, instead of (or in addition to) the tracking of known targets. The need to undertake target discovery in the present circumstances is readily apparent from the increased terrorist threat in Europe, as exemplified by the state of emergency in France following the Paris attacks of November 2015.

80. Further, even where a known target has been identified, the reasonable basis for targeting that individual's communications may not be that they are themselves engaged in planning or committing criminal acts. A person may be a legitimate intelligence target whether or not they are involved in criminality or analogous acts: for instance, an employee of a hostile foreign government, or a person in contact with a terrorist.

81. In this context, the requirements of s.5 of RIPA, as read with the relevant definitions in s.81 of RIPA and with §§6.11-6.12 of the Code are plainly sufficient as recently affirmed by this Court in *RE v United Kingdom* at §133.

(2) The categories of people liable to have their communications intercepted: **§§161-169**

[38] Annex 6 to the Observations.

82. For the reasons set out at §5-29 above it is not correct that the initial interception stage is indiscriminate or "virtually limitless" as sought to be contended for by the Applicants (and whether in terms of communications data or otherwise). Consequently the material differences with the regime in *Weber* are not accepted. As set out at §4.42 of the Observations, the categories of persons liable to have their communications intercepted are sufficiently identified at the interception stage.

83. As regards §167 of the Applicants' further observations:

a. The certificate sets out the categories of communications that GCHQ may examine and the categories directly relate to the intelligence-gathering priorities set out by the Joint Intelligence Committee and agreed by the National Security Council (see ISC Report at §100, 3rd bullet and see also the Code at §6.14).

b. The Commissioner confirmed in his 2013 Report that the certificate is regularly reviewed and is subject to modification by the Secretary of State (see §6.5.43 and also see the evidence of Mr Farr at §80).

c. The oversight of the certificate which is provided by the Commissioner is also made clear in the Code (at §6.14) which states: "*The Interception of Communications Commissioner must review any changes to the descriptions of material specified in a certificate.*"

d. The ISC report also makes clear that the Foreign Secretary was satisfied that "*strategic environmental issues*" reflect a legitimate UK requirement for intelligence (see §103).

e. As stated at §104 of the ISC Report, following a review by the Foreign Secretary, the certificate is reviewed at least annually by the Secretary of State.

In those circumstances there are substantive limitations on the categories of people whose information can be selected for examination.

(3) Limits on the duration of interception: §170

84. It is not accepted that the time limits in s.9(6) of RIPA are "effectively meaningless". There can be no "long-term rolling renewals" of warrants since there are safeguards in place to ensure that any renewals are necessary and proportionate:

a. The application for renewal must be made to the Secretary of State, and must contain all the detailed information set out in §6.10 of the Code, just as with the original warrant application (see §6.22 of the Code[39]). The Code states at §6.22 with regard to the renewal application:

"…the applicant must give an assessment of the value of interception to date and explain why it is considered that interception continues to be necessary for one or more of the statutory purposes in section 5(3), and why it is considered that interception continues to be proportionate."

b. No s. 8(4) warrant may be renewed unless the Secretary of State believes that the warrant continues to be necessary on grounds falling within s. 5(3) RIPA: s. 9(2). Further, by s. 9(3), the Secretary of State must cancel a s. 8(4) warrant if he is satisfied that the warrant is no longer necessary on grounds falling within s. 5(3). Detailed provision is made for the modification of warrants and certificates by s. 10 RIPA.

c. §6.27 of the Code also requires records to be kept of copies of all renewals and modifications of s. 8(4) warrants / certificates, and the dates on which interception is started and stopped (and §5.17 of the 2002 Code was to like effect).

(4) The procedure to be followed for examining, using and storing the data obtained: §§171-178

[39] See also to parallel effect §5.12 of the 2002 Code.

85. The Government's detailed case on this topic is to be found at §§4.51-4.53 of the Observations. In terms of the further criticisms which have been made by the Applicants, the Government responds by making the following key points:

a. There is good reason for s. 16 of RIPA covering access to intercepted material (*i.e.* the content of communications) and not covering access to communications data:

i. In order for s. 16 to work as a safeguard in relation to individuals who are within the British Islands, but whose communications might be intercepted as part of the S. 8(4) Regime, the Intelligence Services need information to be able to assess whether any potential target is "*for the time being in the British Islands*" (for the purposes of s. 16(2)(a)). Communications data is a significant resource in this regard.

ii. In other words, an important reason why the Intelligence Services need access to related communications data under the s. 8(4) Regime is precisely so as to ensure that the s. 16 safeguard works properly and, insofar as possible, factors are not used at the selection that are - albeit not to the knowledge of the Intelligence Services - "*referable to an individual who is ... for the time being in the British Islands*".

b. The programmes referred to at §172 of the Applicants' further observations are neither confirmed nor denied and in any event do not form the subject matter of this application.

c. Whilst it is right that internal communications can be read if they are selected by reference to a factor which is not by reference to an individual known to be in the British Islands, there are extensive safeguards in place to protect against arbitrary interference. Those are set out at §4.52 of the Observations and have been largely ignored by the Applicants. In addition the system ensures that, even if it is subsequently discovered that an individual is

actually in the UK, when previously that was not known, the SIAs must cease all action at that point (see §112(iv) of the ISC Report).

d. As to the suggestion that s.16(3) of RIPA does not provide the same rigour as a s.8(1) warrant, this is not accepted, as explained at §4.44 of the Observations. In addition, David Anderson QC, after investigating the position in detail in his report 'A Question of Trust', concluded as follows at §6.56(a):

"Most UK-based individuals who are subjects of interest to the security and intelligence agencies or law enforcement are however targets of s8(1) warrants issued by the relevant Secretary of State, which will authorise the interception of all their communications, where necessary with the assistance of GCHQ."

e. It is not the case that there is no regulation or oversight of the use of selectors and search criteria:

i. The detail of the s.15 and s.16 RIPA arrangements is kept under review by the Commissioner (see §4.53 of the Observations).

ii. The Code contains express provisions which require records to be kept of the arrangements for securing that only material which has been certified for examination (in accordance with the statutory purposes and tests of necessity and proportionality) is, in fact, read, looked at or listened to (see §6.28 and §§7.16-7.18 in the context of s.16 RIPA). In practice that means that a necessity and proportionality justification must be prepared for any selectors and search criteria which are used.

f. Finally the IPT's Third Judgment dated 22 June 2015 does not support the contention that the procedures for examining, using and storing data are inadequate. That single error does not undermine the overall effectiveness of the safeguards. In addition it is to be noted that the IPT concluded that the "*the selection for examination was proportionate*" (see §15). The Tribunal also indicated that it was "*satisfied that no use whatever was made by the intercepting*

agency of any intercepted material, nor any record retained, and that the Sixth Claimant has not suffered material detriment, damage or prejudice as a result of the breach."

(5) The precautions to be taken when communicating intercepted material to other parties: §§179-181

86. The Applicant's suggestion that there should be a requirement for individualised reasonable suspicion is addressed in detail at §90-97 below.

87. As to the safeguards for the dissemination of intercepted information and any related communications data, it is to be noted that s.15(2) of RIPA is supplemented by the Code and by the constraints imposed by other primary legislation as explained at §4.52(4) and §2.92 of the Observations.

(1) In addition the Applicants have misread *Weber* in the submissions made at §180. At §40 of Weber it was noted that the Federal Constitutional Court had made clear that the transmission of data was proportionate if it served an important legal interest and if there was a sufficient factual basis for the suspicion that "*criminal offences were being planned or had been committed*" (emphasis added). Given that any disclosure under the s.8(4) regime must satisfy the requirements of s.15(2) as supplemented by the constraints imposed by ss. 1-2 of the SSA and ss. 1-2 and 3-4 of the ISA, as read with ss. 19(3)-(5) of the CTA and s. 6(1) of the HRA, there is not a material difference between the s.8(4) regime and the strategic monitoring system in *Weber* in this regard.

(6) The circumstances in which data obtained may or must be erased or the records destroyed: §§182-183

88. The Applicants' case that these safeguards are "unclear" is not understood. For the reasons set out at §4.54 of the Observations this requirement is obviously met.

89. There is also no suggestion in the IPT's Third Judgment of 22 June 2015 that the "technical"[40] retention period error in respect of Amnesty International was a systemic problem. Had that been the case the IPT can be expected to have said so in that judgment. In addition the IPT specifically addressed this in its judgment in *Human Rights Watch v Secretary of State for the Foreign and Commonwealth Office et al* [2016] UKIP Trib 15/165/CH, 16 May 2016, at §44, concluding that:

> *"We are satisfied that there was not... some kind of systemic or wide-ranging failure by the Respondents by virtue of what was disclosed in Liberty/Privacy No 3. There were, as described in paragraphs 5 and 6 above, two relatively minor breaches of procedure."*

Further minimum safeguards? §§184-200

No requirement for individual reasonable suspicion

90. At §§185-187 of their further observations the Applicants assert that there should be a minimum requirement of reasonable suspicion that a sender or recipient has committed an offence. In support of that contention the Applicants rely on *Zakharov* and *Szabo*.

91. The true principle to be derived from the authorities on Article 8 is that any interception of and access to communications must be necessary and proportionate, and must satisfy the *Weber* criteria, which the s.8(4) Regime does: see Observations, §§4.40-4.56. Any attempt to frame a narrower rule which (for example) outlaws any interception, save where a target has already been identified before the interception takes place, is contrary to the whole thrust of the Court's case law, which permits "strategic monitoring": see *Weber,* where the challenge to the German state's regime in this respect was not only dismissed, but declared manifestly ill-founded. The Applicants impermissibly elevate the Court's particular findings on the specific facts

[40] See §14 of the IPT's Third Judgment dated 22 June 2015 where the IPT stated: "*We are satisfied however that the product was not accessed after the expiry of the relevant retention time limit, and the breach can thus be characterised as technical, though (as recognised by the Tribunal in the Belhadj Judgment) requiring a determination to be made. Though technical, the breach constitutes both "conduct" about which complaint may properly be made under section 65 of RIPA and a breach of Article 8 ECHR… The Tribunal is satisfied that Amnesty… has not suffered material detriment, damage or prejudice as a result of the breach, and that the foregoing Open Determination constitutes just satisfaction, so there will be no award of compensation."*

of certain cases into statements of general principle, rather than findings on particular facts in a particular context.

92. The Applicants rely on *Zakharov* to contend that "reasonable suspicion" against an individual is a necessary precondition for any surveillance, because the Court found that *"the authorisation authority's scope of review… must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting the person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures…"*: *Zakharov*, §260.

93. That finding at §260 of *Zakharov,* however, must be seen in its context. It concerned the sufficiency of the authorisation authority's scope of review, where the issue was the propriety of the intelligence agency's request to perform a search operation targeting the communications of a specific individual (see e.g. §§38 and 44 of the judgment). The Court accepted that the requirement for prior judicial authorisation in Russian law was an important safeguard, but found that it was not sufficient in the circumstances, because the domestic court's scrutiny was limited. In particular, the domestic court had no power to assess whether there was a sufficient factual basis for targeting the individual concerned: see §§260-261. Moreover, there was no effective *post facto* judicial scrutiny either: §298. Thus, the totality of the safeguards did not provide adequate and effective guarantees against abuse: §302.

94. In short, the context in *Zakharov* concerned the nature of the available safeguards, where a particular individual had already been targeted; and unsurprisingly, the Court considered that it was important for those safeguards to include effective independent judicial oversight of that targeting decision, capable of assessing its merits.

95. Nothing in *Zakharov* either states or implies that, in order for there to be sufficient safeguards against abuse, any target of surveillance must always be identified in advance on the basis of reasonable suspicion. Rather, the true position on the basis of the Court's jurisprudence is that:

(1) It is the totality of safeguards against abuse within the system that is to be considered. See e.g. *Zakharov* at §§257, 270-271.

(2) Where a decision has been made to target a particular individual, it will be necessary for a judicial authority to be able to review that decision on its merits (i.e. to determine not simply whether it was taken in accordance with proper procedures, but to assess whether it was necessary and proportionate). See *Zakharov*.

(3) However, such judicial oversight can be either *ex ante* or *post facto*: see e.g. *Szabo* at §77, *Kennedy* at §167.

(4) The s.8(4) Regime provides such oversight. It is able to, and will, examine the necessity and proportionality of any interception or examination of the complainant's communications, with the benefit of full access to the evidence. See Observations, §§2.39-2.45.

96. As to the Applicants' reliance on *Szabo*, as the Applicants themselves accept (see §186(2) of the further observations), the Fourth Section's observations at §71 of the judgment were in the context of its proportionality assessment and whether the type of "secret surveillance" which had been undertaken by the TEK had been demonstrated as necessary and proportionate. Again these observations have to be seen in the context of a regime which, it was found, allowed ordering of interception entirely by the Executive, with no assessment of strict necessity, with potential interception of individuals outside the operational range and in the absence of any effective remedial or judicial measures.

97. For the reasons explained at §§13-21 above, the Bulk Powers Review demonstrates that the bulk interception powers in the s.8(4) regime are necessary and proportionate, even where the intelligence services are searching for the communications of individuals who have not already been identified as a target and in order to identify threats to the UK. That does not "obviate" any meaningful

assessment of proportionality as that Review and the case studies referred to therein amply demonstrate.

Prior independent authorisation: §§188-193

98. The suggestion that there should be prior independent authorisation of s.8(4) warrants has been comprehensively addressed at §§4.96-4.99 of the Observations. That this is not a minimum requirement was made expressly clear in *Szabo* at §77. This is a situation in which there is extensive independent (including judicial) *post factum* oversight.

99. Neither *Digital Rights Ireland* or *Tele 2 & Watson* (Advocate General Opinion) are relevant in this context. Neither of those cases lay down definitive mandatory requirements relevant to the present context and the Government reserves the right to make further submissions on the latter case following the judgment from the CJEU.

Subsequent notification of interception measures: §§194-200

100. As to the suggestion that there should be a minimum requirement of subsequent notification to individuals of interception measures:

a. That was not a proposition which was advanced domestically before the IPT in these proceedings.

b. As set out above, the *Szabo* decision has to be read in the context of a regime which was entirely deficient in terms of safeguards of the Executive action in question. The Court reached its determination on the basis that there was a failure to comply with the *Weber* minimum safeguards and it was unnecessary for the Court to embark on the question whether enhanced guarantees were necessary (§70). Accordingly, there was no suggestion that the Court was laying down further minimum requirements over and above the *Weber* minimum criteria and there was no indication in §86 that

subsequent notification of surveillance measures was such a requirement. As the Court noted at §86 it was the *combination* of a complete absence of safeguards plus a lack of notification which meant that the regime could not comply with Art. 8 ECHR.

c. The Opinion of the Advocate General in *Tele 2* & *Watson* does not support the proposition that there should be a minimum requirement of notification. §236 of his Opinion (cited at §195 of the Applicants'' further observations) was addressing the question of supervision by an independent body, not subsequent notification of data retention (or surveillance measures).

d. Finally it is not correct to say that the Commissioner has been "strongly critical" of "unnecessary limitations" on his oversight (see §§199-200 of the Applicants' further observations). The matters set out at §200 of the Applicants' further submissions formed part of a "wish list" of elements which the Commissioner would have like to have seen in the Investigatory Powers Bill 2016 to strengthen the current oversight of surveillance powers. It was not a suggestion that the current s.8(4) regime was unlawful without subsequent notification to individuals of surveillance measures.

Necessity and proportionality of the s.8(4) regime: §201-214

101. At §§201-214 of the Applicants' further observations it is said that the "bulk interception regime" is unnecessary and disproportionate. In this regard the Government repeats §§4.84-4.95 of the Observations and makes the following additional points.

Strict necessity

102. The Court has consistently recognised that when balancing the interests of a respondent State in protecting its national security through secret surveillance measures against the right to respect for private life, the national authorities enjoy a *"fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of*

protecting national security": see e.g. *Weber* at §106, *Klass* at §49, *Leander* at §59, *Malone* at §81.

103. To the extent that the Applicants rely on *Szabo* for the proposition that a test of "strict necessity" is required, it is submitted that the test previously set out by the Grand Chamber and in the other long-standing cases just referred to is to be preferred. It represents a properly protective set of principles which balance both the possible seriousness of the Article 8 interference with the real benefits to the general community of such surveillance in protecting them against acts of terrorism. Strict necessity as a concept is used expressly in the Convention scheme – indicating that it should not be imported elsewhere; or, if that is permissible at all, then only with the greatest caution. There is no warrant for any stricter test in principle in the present context.

104. However, whether viewed through the prism of general necessity, or adopting the test of "strict necessity" in the respects identified in *Szabo*, the s.8(4) Regime satisfies the necessity test.

The necessity and proportionality of the s.8(4) regime

105. The rationale for the s.8(4) Regime and its operation have been addressed on a number of occasions by independent bodies, viz. the IPT, the ISC, the Commissioner, the Anderson Report, and the Bulk Powers Review. Materially, the Anderson Report, the Bulk Powers Review and the ISC in its report of 17 March 2015 (the ISC Report) all conclude in terms, and with supporting analysis and detail, that less intrusive (or different) programmes could not address legitimate needs of the UK. See above and Observations, §§1.21-1.35.

106. Although it is correct that the Independent Reviewer in the Bulk Powers Report was not specifically tasked with opinion on whether bulk interception powers were proportionate (see §204 of the Applicants' further observations), the conclusions of that review and plainly highly material to that question, as summarised at §§13-21 above. At §§9.12-9.14 he stated:

"I have already summarised what I consider to be the strength of the operational case for each of the bulk powers (chapters 5-8 above). Among the other sources of evidence referred to in chapter 4 above, I have based my conclusions on the analysis of some 60 case studies, as well as on internal documents in which the SIAs offered frank and unvarnished assessments of the utility and limitations of the powers under review.

The sheer vivid range of the case studies – ranging from the identification of dangerous terrorists to the protection of children from sexual abuse, the defence of companies from cyber-attack and hostage rescues in Afghanistan – demonstrates the remarkable variety of SIA activity. ***Having observed practical demonstrations, questioned a large number of analysts and checked what they said against contemporaneous intelligence reports, neither I nor others on the Review team was left in any doubt as to the important part played by the existing bulk powers in identifying, understanding and averting threats of a national security and/or serious criminal nature, whether in Great Britain, Northern Ireland or further afield.***

My specific conclusions, in short summary, are as follows:

(a) ***The bulk interception power is of vital utility across the range of GCHQ's operational areas, including counter-terrorism, cyber-defence, child sexual exploitation, organised crime and the support of military operations. The Review team was satisfied that it has played an important part in the prevention of bomb attacks, the rescuing of hostages and the thwarting of numerous cyber-attacks. Both the major processes described at 2.19 above [i.e. the "strong selector" and "complex query" process] produce valuable results. Communications data is used more frequently, but the collection and analysis of content has produced extremely high-value intelligence, sometimes in crucial situations. Just under 50% of GCHQ's intelligence reporting is based on data obtained under bulk interception warrants, rising to over 50% in the field of counter-terrorism."*** (emphasis added)

107. In the light of the conclusions of this review, to describe the Government's bulk interception as "*a speculative fishing exercise, designed to check the behaviour of an entire population*" (see §212 of the Applicants' further observations) could not be further from the truth. It is a capability which is of "*vital utility*" in identifying, understanding and averting threats of a national security and/or serious criminal nature.

108. As to the Applicants' reliance on cases involving the bulk *retention* of data (see §§203, 207-209 of the Applicants' further observations), those are irrelevant to the issues raised in this application which involves bulk interception followed by

targeted selection of material. This is not a situation where there is bulk retention of data on an "indiscriminate" basis (see §§207-208 of the Applicants' further observations).

109. Finally it is the case that the bulk interception process involves the discarding of unwanted communications and it does not permit "*the storing and analysing of collateral data*" (see the Applicants' further observations at §213). That was made clear in the Bulk Powers Review at §§2.16 and 2.17. The second (filtering) stage involves discarding those bearers least likely to be of intelligence value and the third (selection) stage involves automatically discarding all communications that do not match the chosen selection criteria.

The lawfulness of the intelligence sharing regime: §§232-250

110. At §§232-250 of the Applicants' further observations it is submitted that "*the standards applicable to interception*" under Art 8 ECHR should also apply "*when access is given to intercepted material even if the actual initial interception was carried out by a foreign intelligence service*"[41].

111. The assertion that the *Weber* safeguards should apply to the sharing of intelligence between the US and UK is misguided, for reasons set out in the Observations at §§3.29-3.36. In short summary:

a. There is no Article 8 case of the Court suggesting that the *Weber* criteria should be applied in the distinct factual context where the intelligence agencies of the respondent State have merely obtained information from a foreign State.

b. The Court has expressly indicated that the "rather strict standards" developed in recent Strasbourg intercept cases do not necessarily apply in other intelligence-gathering contexts[42].

[41] See, in particular, §243.
[42] See Observations at §3.32.

c. There is no good reason to single out intercepted communications/communications data from other types of information that might in principle be obtained from a foreign intelligence agency, such as intelligence from covert human sources or from surveillance. In many cases, the Intelligence Services may not even know whether information from an intelligence agency does derive from interception. Moreover, there is no particular reason why such information should be more sensitive than information from any other source. But it would not plainly be neither feasible nor (from a national security perspective) safe for a domestic legal regime to set out all the various types of intelligence that might be obtained from a foreign State; define the tests to be applied when determining whether to obtain them, and the limits on access; and set out the handling, etc. requirement and the uses to which all such types of information might be put.

112. This is not to place form over substance (see §§235-236 of the Applicants' further observations). As Mr Farr explains, neither the sensitivity of the information in question, nor the ability of a person to predict the possibility of an investigative measure being directed against him, distinguish communications and communications data from other types of intelligence: Mr Farr §§27-30. Thus, it would be nonsensical if Member States were required to comply with the *Weber* criteria for receipt of intercept material from foreign States; but were not required to do so for any other type of intelligence that foreign States might share with them.

113. There is also no contradiction in the Government's policies, including in the Code. Whilst the Government has been able to formulate rules for the requesting and handling of intercepted communications content or data from a foreign state (irrespective whether it is solicited or unsolicited, analysed or unanalysed, and whether or not the communications data is associated with the content of communications) (see §239-240 of the Applicants' further observations), that does not mean that it would be feasible to formulate rules for all the different types of information which might be shared by foreign governments. If the *Weber* criteria apply to the obtaining of intercept material from a foreign intelligence agency, and if

the intelligence sharing regime does not satisfy those criteria, then it is difficult to see how the Intelligence Services could lawfully obtain any information from a foreign intelligence agency about an individual that derived from covert human intelligence sources, covert audio/visual surveillance or covert property searches. But that would be a remarkable, and deeply concerning, conclusion - not least given that intelligence sharing is (and has for many years been) vital to the effective operation of the Intelligence Services (see Mr Farr §§15-26).

114. As to the suggestion that the intelligence sharing regime was substantively defective prior to December 2015 (as well as being insufficiently signposted in public) (see §§246-247 of the Applicants' further observations), for the reasons set out at §§90-99 above, there is no requirement for prior judicial authorisation or any requirement for individual reasonable suspicion.

115. In terms of the Disclosure which was recorded in the IPT's 5 December and 6 February Judgments (see §248 of the Applicants' further observations), since it formed part of a judicial decision it can be taken into account in assessing "forseeability" for Art. 8(2) ECHR purposes – see the Observations at §2.23 and footnote 63. Therefore, prior to being incorporated into the Code, the domestic position was the same as a result of the 5 December and 6 February judgments.

116. It is also inaccurate to speak merely of a "note" setting out the Government's policy. The substance of the note was reflected in the IPT's judgments and is now set out in the Code, which is itself "law" for the purposes of the "in accordance with the law" requirement (see e.g. *Kennedy* and §3.38 of the Observations). In any event the Disclosure is also "law" for these purposes: it is a published statement, contained in publicly accessible court judgments.

117. Finally there is no merit in the criticism that the Disclosure (as now reflected in Chapter 12 of the Code) is obscurely drafted or vague (see §248(2)-(4) of the Applicants' further observations).

a. It is clear that the terms "request" and "receipt" would cover all the scenarios where the SIA that carry out the relevant activities can access material intercepted by foreign intelligence agencies in the circumstances mentioned in §248(2). The access to databases or raw material referred to at §248(2) of the Applicants' further submissions would, on a straightforward application of the Code, be covered by it.

b. The concepts of "analysed" and "unanalysed" are also sufficiently clear (§248(3)). They are ordinary English words, which require no further definition. Material which has been automatically scanned and selected, but which has not been examined, is "unanalysed"; and material which has been examined, and conclusions drawn about it in the form of a report or analysis, is "analysed".

c. It is wrong to suggest that there is no protection for communications data (§248(4)). As set out at §12.6 of the Code where communications content or communications data (and whether or not the data is associated with the content of communications) are obtained by the intercepting agencies or otherwise received from a government of another state in circumstances where the material identifies itself as the product of an interception, it must be subject to the same internal rules and safeguards that apply to the same categories of content or data when they are obtained directly by the intercepting agencies as a result of interception under RIPA.

Victim Status

118. The Government does not repeat the submissions about victim status made at §§3.2-3.6 and §4.1 of the Observations. For the avoidance of doubt the Government made clear in its Observations that it was accepted that the South African Legal Resources Centre and Amnesty International did satisfy the victim test in the context of the s.8(4) regime – see §4.1 of the Observations and see §255 of the Applicants' further observations.

119. As regards the intelligence sharing regime, the US programmes referred to at §256 of the Applicants' further submissions, which are said to operate under Executive Order 12333, do not form the subject-matter of this application, which is specifically limited to the Prism and Upstream programmes (which are authorised under s.702 of FISA). In those circumstances it is impermissible for the Applicants to seek to rely on those programmes in support of the contention that they are victims for the purposes of the intelligence sharing regime complaints.

Article 14 ECHR: §§262-271

120. This is addressed in detail at §§8.1-8.16 of the Observations.

121. In terms of whether there is a relevant difference of treatment:

a. It is not the case that the IPT came to the conclusion that the s.16 safeguards have a "disproportionately prejudicial effect" on non-British nationals (see §266 of the Applicants' further observations). That was the *submission* which was made to the IPT by the Applicants, as recorded at §144 of the First Judgment (5 December 2014). But the IPT did not have to determine that submission, because it reached the very clear conclusion that any difference in treatment could, in any event, be justified (see §148 of the First Judgment and the reference to "*any indirect discrimination is sufficiently justified*"). In those circumstances the Government is not seeking to challenge a finding which was made by the IPT in this regard (as suggested at §§265-266 of the Applicants' further observations).

b. As regards the Applicants' analysis of *Magee v United Kingdom*[43], including with reference to *Carson v United Kingdom* App. No. 42184/05, 16 March 2010, any difference in treatment is not on the grounds of "residence" (see §70 of *Carson*), but on the grounds of current location. That is not a relevant difference of treatment for the purposes of Art. 14 ECHR.

[43] App. No. 28135/95, ECtHR 6 June 2000

122. On the question of justification (even if there is (which is denied) a relevant different of treatment), the Applicants' further observations (§§270-271) can be answered as follows:

a. The field of national security is a paradigm example of where a state's margin of appreciation is wide – see *Weber* at §106, *Klass* at §49, *Leander* at §59, *Malone* at §81. The *Stec* test is not inappropriate in the present context (see §271(3) of the Applicants' further observations);

b. The factors relied upon by the Government in support of any difference in treatment were compelling and obvious and are not in any way diminished by a lack of witness evidence to support them. It was "*quite plain*" to the IPT that "*the imposition of a requirement for a s.16(3) certificate in every case would radically undermine the efficacy of the s.8(4) regime, given the pre-eminent role of that regime in the identification of threats to UK national security from abroad*" (§148 of the First (5 December 2014) judgment). There is no proper basis for this court departing from that conclusion of the expert domestic tribunal in this area.

c. There is no inconsistency between the Government's case and its explanation of how the s.8(4) regime works. As set out at §16 above, the selection stage of the s.8(4) process may involve "strong selectors" but it can also involve the "complex query" process. In many cases the SIAs will not know who the individual is and that is wholly unsurprising given the current nature of the terrorist threat which the UK faces – as discussed at §§8.14-8.16 of the Observations.

d. Finally the distinction is not irrational for the reasons explained at §§8.13-8.16 of the Observations. The Government has a panoply of powers to investigate a person present in the UK and that distinction justifies any relevant difference in treatment.

Article 6 ECHR

Determination of civil rights and obligations

123. The suggested distinctions which are asserted by the Applicants at §§272-277 of the Applicants' further observations are unsustainable. In determining whether Art. 6(1) applies to the Applicants' complaints it cannot be relevant whether a domestic tribunal already exists or not. The question is whether the supervisory measures in question are within the scope of the definition of 'civil rights' in Art. 6(1). As recognised by the Grand Chamber in *Ferrazzini* at §24[44], that concept is "autonomous" and thus it cannot be interpreted solely by reference to the domestic law of the respondent State. In addition the Tribunal is specifically designed to operate under the constraints recognised by the Court at §57 of *Klass* (and upon which the Court's conclusion in *Klass* under Art. 6 was based). In particular, a complainant in the Tribunal is not permitted to participate in any factual inquiry that the Tribunal may conduct into the allegations that he has made: eg. the fact of any interception remains secret throughout (save, of course, where the Tribunal finds unlawfulness to have occurred). Thus the fact that RIPA offers individuals the additional safeguard (under Art. 8) of an unlimited right to complain to the Tribunal cannot in itself make Art. 6 apply to such disputes.

124. In *Klass* the Commission reached the clear conclusion that Art. 6 does not apply to state interference on security grounds and there is no good reason why that should not apply in this context. That approach is entirely consistent with the Court's more general jurisprudence on the meaning of "civil rights and obligations" for the reasons set out at §§7.6-7.8 of the Observations.

Fairness

125. The Applicants have raised two new matters which they say are relevant to the assessment of whether the IPT proceedings were compliant with Art. 6(1) ECHR (assuming it applied). They rely on the 28 September 2007 meeting at Thames House (see §§281-283 and also §§98-100 of the Applicants' further observations) and they

[44] App. No. 44759/98, 12 July 2001

also rely on the administrative error which the IPT initially made in its Third Judgment when it mistakenly attributed a finding on breach of Art 8 ECHR to the wrong complainant.

126. In terms of the meeting of September 2007 (recorded in a Note for File dated 15 November 2007) this has been addressed at §§56(b)-(d) above. There is no merit in the suggestion that this undermines the independence or effectiveness of the IPT nor can there be any sensible suggestion that the searches which were conducted in this case were not reasonable or proportionate.

127. As to the reliance on the error made by the IPT, the IPT made clear in its letter dated 1 July 2015 that there had been a mistaken attribution in the judgment which arose after all judicial consideration had taken place and did not result from any failure by the Respondents to make disclosure. That is not a matter which can appropriately lead to the criticism that it demonstrates a lack of rigour in the Tribunal's proportionality assessment. The IPT's judgment (including its proportionality assessment) was reached after full consideration of the relevant material in closed sessions, where the applicants' interests were represented by CTT.

Article 10 ECHR

128. The Article 10 ECHR aspect of the complaints has been addressed in detail at §§6.2-6.39 of the Observations. In response to the Applicants' further observations at §§286-294, the Government makes the following key points:

a. It is to be noted that it was agreed between the parties during the IPT proceedings that, save for the question of prior judicial authorisation, no separate argument arose in relation to Article 10(2), over and above that arising under Article 8(2) (see the IPT's First Judgment dated 5 December 2014 at §149).

b. The Applicants rely on *Sanoma Uitgevers BV v The Netherlands*[45] (see §290 of their further observations), but that was a case concerned with targeted measures to compel disclosure of journalistic sources rather than a regime of strategic monitoring in the course of which journalistic (or NGO) material might be intercepted (*Weber*). It was in that context that the Court identified the importance of prior authorisation by a Judge or other independent body.

c. It is not correct to characterise the relevant provisions of the Code (which do not exhaustively define "confidential communications") as "*nothing more than restatements of "considerations" which may be taken into account*" (see §293 of the Applicants' further observations). As set out at §6.26 of the Observations the Code provides for a series of practical steps which must be taken in terms of the retention, destruction, handling and dissemination of confidential information and that includes notifying the Commissioner of any such material which is retained and making any such information available to him on request.

d. As to proportionality and necessity, the Applicants do not explain how it would be practical or feasible to screen out human rights NGO's privileged communications from the collection stage of the s.8(4) interception regime. It is also material to note that the IPT was entirely satisfied that the communications of Amnesty and the South African Legal Resources Centre had been "lawfully and proportionately" intercepted and accessed/selected for examination (see §§14-15 of the Third Judgment dated 22 June 2015). The effect of the Applicants' submissions is that it could never be necessary or proportionate to subject human rights NGO's communications to s.8(4) activity or the intelligence sharing regime and that is contradicted by the specific findings which the IPT made in these cases.

JUST SATISFACTION – PARA 24

[45] [2011] EMLR 4

129. The Government notes that the Applicants' position is that a reasoned finding of breach of the Convention would be sufficient just satisfaction and they do not seek their costs (see §24 of the Applicants' further observations). In those circumstances it is unnecessary for the Government to make any substantive submissions on this topic.

II REPLY TO INTERVENORS' SUBMISSIONS

European Network of National Human Rights Institutions ("ENNHRI")

Article 6 ECHR: §§8-17

130. ENNHRI's submissions on Article 6 ECHR proceed on a fundamental misunderstanding of what occurred in the domestic IPT proceedings. In particular:

a. The IPT did not "refuse" to direct disclosure of the SIA's sensitive internal guidance concerning the treatment of NGO material. As set out in detail at §§7.37-7.38 of the Observations, the IPT reasonably and appropriately concluded that the issue of NGO confidence had been raised far too late in the domestic proceedings to be considered and the IPT cannot properly be criticised for taking that approach.

b. The IPT did not refuse to consider the Respondents' NCND policy. By agreement between the parties that issue did not arise for determination by the Tribunal (see §13 of the First Judgment dated 5 December 2014).

c. It is not correct to state that the Applicants were not represented in the closed hearing – as explained at §§7.43-7.44 of the Observations the Applicants had the benefit of CTT who was instructed to represent their interests during the closed hearing. Overall there was no unfairness in the procedures which were adopted.

d. In addition, CTT was able to make submissions on the sensitive arrangements which were relevant to the complaints.

131. At §§12 of ENNHRI's submissions it is said that the proceedings in the IPT must have involved the determination of "civil rights" because this was a situation whereby a "judicial body was entrusted with a judicial task". This has been addressed at §119 above. The fact that RIPA offers individuals the additional safeguard (under Art. 8) of an unlimited right to complain to the Tribunal cannot in itself make Art. 6 apply to such disputes.

132. For the reasons set out in detail at §§7.11-7.50 of the Observations, even if Art. 6(1) did apply to the IPT proceedings, those proceedings were fair. To the extent that it is suggested at §16 of ENNHRI's submissions that proceedings could never be fair (whether under the ICCPR or the ECHR) in circumstances where a party is not provided with full disclosure, that is in direct conflict with the decision in *Kennedy v United Kingdom*, where the Court held that the need to keep secret sensitive and confidential information justified the strong restrictions on disclosure of relevant information in proceedings before the IPT in the UK (see §§7.26-7.31 of the Observations). The decision in *ZZ (France) v SSHD*[46] (relied upon by ENNHRI at §17) also acknowledges the possibility of derogation from disclosure requirements for reasons of national security: see §§57-59 and §§64-69. It is not authority for the proposition that there could never be circumstances in which sensitive material was considered in the absence of a party to proceedings.

Article 10: §§18-30

133. The relevance of the case law and other sources cited at §§22-26 of ENNHRI's submissions is not understood. This is not a situation where there has been punishment, prosecution/imprisonment or suppression of journalists or NGOs, nor can it sensibly be suggested that this jurisprudence applies "indirectly" (see §28 of ENNHRI's submissions).

[46] Case C-300/11

134. In terms of the definition of "national security" (see §24 & §27 of ENNHRI's submissions), for the reasons set out at §§4.77-4.81 of the Observations that concept is not "amorphous" in the way it applies to the to the s.8(4) regime, which is designed to ensure that a person's communications cannot be examined simply by reference to unparticularised concerns of "national security". Further, the s.8(4) regime does have precisely those checks and balances to prevent misuse which are called for at §29 of ENNHRI's submissions, for the reasons set out at §§4.32-4.83 and §§6.2-6.30 of the Observations and §§62-89 above.

135. The s.8(4) regime is also proportionate (whether under Art 8 or Art 10 ECHR) for the reasons explained at §§4.84-4.95 and at §§101-109 above.

Article 14: §§31-38

136. As to ENNHRI's submissions on Article 14 ECHR:

a. This is not a situation where there is discrimination on the grounds of nationality. Any difference in treatment is on the grounds of current location and that is not a relevant difference of treatment for the purposes of Art. 14 ECHR, as explained at §§8.3-8.5 of the Observations and at §121 above.

b. In addition, even if there is a relevant difference of treatment (which is not admitted) it is clearly justified for the reasons given at §§8.7-8.16 of the Observations and at §122 above. It is to be noted that ENNHRI's submissions do not attempt to engage with the rational justification for any difference of treatment which is relied upon by the Government and which was straightforwardly accepted by the IPT in its First Judgment of 5 December 2014 – see §§141-148 of the First Judgment dated 5 December 2014.

Electronic Privacy Information Centre ("EPIC")

137. The EPIC submissions make wide-ranging and inaccurate submissions about the nature of US surveillance and US Surveillance law. It is unnecessary and

inappropriate for the Court to make findings about that law (or indeed any future developments in it) in this Application.

138. The EPIC submissions also address alleged US surveillance activities outside the scope of this Application. The Application is about the UK's alleged receipt of information from the USA's PRISM and Upstream programmes, which the NSA operates under the authority of s.702 FISA[47]. EPIC's submissions address the NSA's surveillance activities under a completely different authority (Executive Order, "EO" 12333). It is unnecessary and inappropriate to address EO 12333.

139. It is also unnecessary to address any US activities under s.215 of the US Patriot Act. As set out at §65 above and at §1.7 of the Observations, any activities under that power are of no relevance to this application.

140. As to the allegation that the Upstream and Prism programmes (governed by s.702 FISA powers) are "*largely ignored by US oversight bodies*" and lack legal protections for non-US persons (see §§12-13 of EPIC's submissions), that is not accepted. The Government repeats the submissions made at §§40-52 above. In addition:

141. The US Government's authority to collect "foreign intelligence information" under s.702 of FISA is limited by a number of requirements which have to be examined together to appreciate the limits on this activity.

a. **First**, whilst the definition of "foreign intelligence information" in s. 702 includes "*information with respect to a foreign power or foreign territory that relates to . . . the conduct of the foreign affairs of the United States*" (see 50 U.S.C.

[47] See e.g. Application §4: "*The two programmes which are challenged by this Application are:*
4.1 The soliciting or receipt and use by the UK intelligence services ("UKIS") of data obtained from foreign intelligence partners, in particular the US National Security Agency's "PRISM" and "UPSTREAM" programmes (herafter "receipt of foreign intercept data"), and
4.2 The acquisition of worldwide and domestic communications by the Government Communications Headquarters ("GCHQ")…"
(Emphasis added).

§1801(e))[48], the US may only target specific non-US persons located outside of the US who possess or who are likely to communicate foreign intelligence information that is tied to a specific topical certification issued by the US Attorney General and the US Director of National Intelligence and approved by the Foreign Intelligence Surveillance Court (FISC or FISA Court).

b. More specifically, as part of the US government's application to the FISC, the Attorney General and Director of National Intelligence must specify the categories of foreign intelligence information that the US government is seeking to acquire.[49] And before the certification can be approved, the FISC must determine that the identified categories of foreign intelligence information intended to be collected by the certifications meet the statutory definition of foreign intelligence information.[50] FISC opinions also make clear that s. 702 collection is targeted and must be specifically tied to an identifiable certification. [51]

c. **Secondly**, collection activities under s. 702 must be targeted in the manner described at §§40-52 above.

d. The targeting procedures protect the privacy of non-US persons by ensuring that each individual targeting decision is based upon a sufficient nexus to the

[48] Specifically, 50 U.S.C. § 1801(e) provides:

(e) "Foreign intelligence information" means--

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against--

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to--

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

[49] *See* the July 2014 report on s.702 by the Privacy and Civil Liberties Oversight Board (PCLOB), an independent executive branch agency (hereafter the PCLOB Report), at 23.

[50] *See* PCLOB Report at 6.

[51] *See* FISC Opinion by Judge Hogan reauthorizing certification in 2014. https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.

foreign intelligence information sought to be obtained by one of the FISC-approved certifications. Similarly, the written certification approved by the FISA Court must include minimization procedures. The minimization procedures for s.702 have been publicly released.[52] These procedures focus on US persons but also provide important protections to non-US persons.

e. For example, communications acquired under s. 702, whether of US persons or non-US persons, are stored in databases with strict access controls. The data may be reviewed only by intelligence personnel who have been trained about the minimization procedures and who have a reason to access the data.[53] The data can only be queried to identify foreign intelligence information or, in the case of the FBI only, evidence of a crime.[54] The minimization procedures (and PPD-28, discussed below) limit how long data acquired pursuant to s. 702 may be retained.[55] Further, the information may be disseminated only if there is a valid foreign intelligence or law enforcement purpose; the mere fact that one party to the communication is not a US person is insufficient.[56] Moreover, NSA's s. 702 minimization procedures state that non-US person communications may only be retained, used, and disseminated "*in accordance with other applicable law, regulation, and policy*."

[52] The minimization procedures are available at http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf; http://www.dni.gov/files/documents/ppd-28/2014%20FBI%20702%20Minimization%20Procedures.pdf; and http://www.dni.gov/files/documents/ppd-28/2014%20CIA%20702%20Minimization%20Procedures.pdf.

[53] *See* NSA Report at 4.

[54] *See, e.g.*, NSA Minimization Procedures at 6-7, *available at* http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf.

[55] *See* NSA Minimization Procedures, *supra* n. 29; PPD-28 Section 4.

[56] FBI PPD-28 procedures available at http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties. *See also* "USSID SP0018: Supplemental Procedures for the Collection, Processing, Retention and Dissemination of Signals Intelligence Information and Data Concerning Personal Information of Non-United States Persons" (January 12, 2015) (NSA PPD-28 Implementation Procedures).

f. **Thirdly**, collection activities under s. 702 are limited to specific and defined intelligence priorities set by policy-makers.[57] These priorities include topics such as nuclear proliferation, counterterrorism, and counter-espionage.

g. **Finally**, collection activities conducted pursuant to s.702 must comply with the privacy protections afforded to non-US persons by Presidential Policy Directive 28 (PPD-28) - see §§1.13-1.14 of the Observations (and see also the Litt Letter). This extends certain protections afforded to the personal information of U.S. persons to non-U.S. person information[58]. It explicitly provides that the personal information of non-U.S. persons acquired during the US' signals intelligence operations shall be afforded privacy protections comparable to the protections afforded to US persons. PPD-28 and IC elements' implementing procedures are publicly available. For example, the NSA Supplemental PPD-28 Procedures state that the United States Signals Intelligence System (USSS) must, "*[w]henever practicable, use one or more selection terms in order to focus collection on specific foreign intelligence targets (e.g., a specific, known international terrorist or terrorist group)*" and the procedures further provide that the USSS "*may not disseminate [personal information of a non-US person] solely because of a person's foreign status*."[59] Additionally, subject to only limited exceptions, NSA is prohibited from retaining information collected pursuant to its signals intelligence activities for more than five years. Section 4(a)(i) of PPD-28.

142. In those circumstances the assertion that US Law does not provide adequate oversight or protection for the collection of non-US persons' data (see §§11-13, §19 and §28-30 of EPIC's submissions) is simply untrue.

Global Campaign for Free Expression (Article 19)

[57] *See* Letter from Robert Litt, General Counsel of the Office of the Director of National Intelligence, dated Feb. 22, 2016, at 4-6 (Annex VI to the Privacy Shield documents) (http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-6_en.pdf) (Litt Letter), discussed below.

[58] NSA's unclassified and publicly available PPD-28 procedures apply to all of NSA's signals intelligence activities, including activities undertaken under s.702 - *see, e.g.*, NSA PPD-28 Implementation Procedures, Section 7.2.

[59] *See* Sections 4.2 and 7.2 of NSA PPD-28 Implementation Procedures.

143. Article 19's submissions are premised on the erroneous basis that the UK SIA's engage in the "*indiscriminate interception, storage and analysis of online communications*" (see §3). As explained in the Observations and at §§5-21 above, that is an inaccurate description of the s.8(4) regime.

144. As to Article 19's submissions at §§4-6, it is to be noted that the Government has accepted (at 6.1 of the Observations) that NGOs engaged in the legitimate gathering of information of public interest in order to contribute to public debate may properly claim the same Art. 10 ECHR protections as the press. In principle, therefore, the obtaining, retention, use or disclosure of the applicants' communications and communications data may potentially amount to an interference with their Art. 10 rights, at least where the communications in question are quasi-journalistic ones, relating to their role as "social watchdogs".

145. As set out in more detail in the Government's Observations (§§6.2-6.9), the principles to be applied regarding the Applicants' Article 10 challenge are materially the same as those relevant to the Article 8 question. The Government reiterates the Court's finding to this effect in *Telegraaf Media* (§90), where it held that the essential requirements of lawfulness were the same for both articles, and observed that the two apparently different provisions ("*in accordance with the law*" in Article 8 and "*prescribed by law*" in Article 10) were identical in the French text of the Convention (where both require that interference be "*prevue(s) par la loi*", §89).

146. Despite Article 19's detailed submissions to the effect that bulk interception might have a chilling effect on the freedom of NGOs and the press (see §§10-14) the proper and proportionate response to these concerns is not, as Article 19 would appear to suggest, a prohibition on bulk interception. It is to ensure that any interception of journalistic or NGO material, if and when that occurs through the operation of the s.8(4) interception regime, be subject not only to the statutory safeguards enshrined in RIPA which apply to all intercepted data (*inter alia*, the requirement of certification with explicit justification, limitations on duration of

interception and disposal of material), but be subject also to the enhanced safeguards set out in the Code.

147. In terms of the submissions at §§15-24 of Article 19's intervention and the particular reliance placed on the September 2014 report of the UN Special Rapporteur, his call for states to justify "*with particularity*" the tangible counter-terrorism advantages which had accrued from "*mass surveillance technology*" was based on extremely broad assumptions about the type of activity which might be taking place (including in the US), which does not accurately reflect the s.8(4) regime[60].

148. Similarly, the reports relied upon at §§25-27 of Article 19's submissions, which, in large part address indiscriminate, untargeted, secret collection of data under "mass surveillance programmes" bear no relation to the s.8(4) regime, as properly understood. The *Digital Rights Ireland* case is also irrelevant for the reasons set out at §§4.17-4.27 of the Observations.

149. The assertion that surveillance must be targeted and based on reasonable grounds for suspicion (with particular reliance on *Zakharov v Russia*) has been addressed at §§90-97 above and those submissions are not repeated.

150. The suggestion that there should be prior independent authorisation of s.8(4) warrants has been comprehensively addressed at §§4.96-4.99 of the Observations. That this is not a minimum requirement was made expressly clear in *Szabo* at §77. This is a situation in which there is extensive independent (including judicial) *post factum* oversight.

Anna McLeod

[60] For example, his reference to collecting "*all communications all the time indiscriminately*" (at §18, p7) and "*the systemic interference with the Internet privacy rights of a potentially unlimited number of innocent people located in any part of the world*" (at §59, p21) are not a fair or accurate characterisation of the s.8(4) regime.

Anna McLeod

Agent of the Government of the United Kingdom

16 December 2016

DECLARATION OF SCOTT BRADNER

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Appendix FF

Application No. 58170/13

IN THE EUROPEAN COURT OF HUMAN RIGHTS

BETWEEN:

10 HUMAN RIGHTS ORGANISATIONS

Applicants

-and-

THE UNITED KINGDOM

Respondent

THE UNITED KINGDOM'S OBSERVATIONS ON THE MERITS

Glossary

The Anderson Report	*A report of June 2015 by the Investigatory Powers Review, conducted by David Anderson QC, entitled "A Question of Trust"*
The British Islands	*The UK, the Channel Islands and the Isle of Man (see s. 5 of and Sch. 1 to the Interpretation Act 1978) (See **Annex 59**)*
The CJEU	*Court of Justice of the European Union*
The Code	*The current Interception of Communications Code of Practice, issued on 15 January 2016 under s. 71 of RIPA*
The 2002 Code	*The previous version of the Interception of Communications Code of Practice, issued in July 2002*
The Commissioner	*The Interception of Communications Commissioner, appointed under s. 57(1) RIPA; currently Sir Stanley Burnton*
Communications data	*Certain data, as per the definition in ss. 21(4), 21(6) and 21(7) of RIPA, that relates to a communication but does not include its contents*
CSP	*Communications Service Provider*
The CTA	*The Counter-Terrorism Act 2008*
The DPA	*The Data Protection Act 1998*
The Disclosure	*The disclosure of certain internal safeguards within the Intelligence Sharing and Handling and s.8(4) regimes, given by the respondents in the Liberty proceedings, and recorded by the IPT in its 5 December and 6 February Judgments.*
DRIPA	*Data Retention and Investigatory Powers Act 2014*
External communication	*A communication "sent or received outside the British islands" (see s. 20 of RIPA, and §6.1 of the Code)*
FISA	*The USA's Foreign Intelligence Surveillance Act 1978*
GCHQ	*The Government Communications Headquarters*
The HRA	*The Human Rights Act 1998*
The Intelligence Services	*As per the definition in s. 81(1) of RIPA: the Security*

	Service, SIS and GCHQ
The Intelligence Sharing Regime	*The regime (set out in "Domestic Law and Practice") that governs the sharing of intelligence between the Intelligence Services and foreign intelligence agencies, and the handling and use of intelligence obtained as a result, in the context of the allegations made by the Applicants (i.e. allegations about the receipt of intelligence from the Prism and Upstream programmes)*
Intercepted material	*In relation to an interception warrant, "the contents of any communications intercepted by an interception to which the warrant relates" (see s. 20 of RIPA)*
An interception warrant	*A warrant issued in accordance with s. 5 of RIPA*
Internal communication	*A communication that is not an external communication*
The IPT	*The Investigatory Powers Tribunal*
The IPT's 5 December Judgment	*The judgment of the IPT of 5 December 2014 in the Liberty proceedings*
The IPT's 6 February Judgment	*The judgment of the IPT of 6 February 2015 in the Liberty proceedings*
The IPT's 22 June Judgment	*The judgment of the IPT of 22 June 2015 in the Liberty proceedings*
The ISA	*The Intelligence Services Act 1994*
The ISC	*The Intelligence and Security Committee of Parliament*
The ISC Report	*A report of 17 March 2015 by the ISC, "Privacy and Security: a Modern and Transparent Legal Framework"*
The ISC's Statement of 17 July 2013	*A statement made by the ISC following an investigation into*
The JSA	*The Justice and Security Act 2013*
The Liberty proceedings	*Proceedings in the IPT brought in 2013 by Liberty, Privacy, Amnesty International and various other civil liberties organisations, challenging the Intelligence Sharing and s.8(4) Regimes, in the same factual premises as are relevant to the present application*
The NSA	*The National Security Agency*
The NSC	*The National Security Council*
The OSA	*The Official Secrets Act 1989*

RIPA	*The Regulation of Investigatory Powers Act 2000*
The Rules	*The Investigatory Powers Tribunal Rules 2000, SI 2000/2665*
A s. 8(1) warrant	*An interception warrant that complies with s. 8(2)-(3) of RIPA*
The s. 8(4) Regime	*The statutory regime (set out in "Domestic Law and Practice") that governs the interception of external communications and the handling and use of the intercepted material and communications data obtained as a result*
A s. 8(4) warrant	*An interception warrant issued under the s. 8(4) regime that complies with ss. 8(4)-(6) of RIPA*
The s.16 arrangements	*the safeguards applying under s.16 RIPA to the examination of intercepted material gathered under a s. 8(4) warrant*
SIS	*The Secret Intelligence Service*
The SSA	*The Security Service Act 1989*

Contents ***Pages***

INTRODUCTION AND EXECUTIVE SUMMARY

1. This Application challenges the United Kingdom's legal regimes governing (i) the receipt of intercept material from the US authorities under the US Government's "Prism" and "Upstream" programmes (the "Intelligence Sharing Regime"); and (ii) the "bulk" interception of communications under s.8(4) of the Regulation of Investigatory Powers Act ("RIPA") (See Annex 1), pursuant to the alleged "Tempora" interception operation ("the s.8(4) Regime"). The detail of the answers given by the Government to these challenges is set out in the body of the Observations below. The level of detail required has inevitably lengthened the Observations. Accordingly, this Executive Summary indicates both the structure of the Observations and provides a summary of the key points made in them given.

2. This is an application of the utmost importance to the UK. It is also of paramount importance to Council of Europe States who benefit from intelligence sharing arrangements with the United Kingdom or have similar legislative provisions governing the lawful interception and surveillance of communications. The information and intelligence obtained under both the Intelligence Sharing Regime and the s.8(4) Regime have been and remain critical to the proper protection of national security, notably against the serious threat from terrorism. Recent events across Europe, including the recent terrorist attacks in Paris and Brussels, and a number of thwarted terrorist plots[1], have emphasised in the clearest way the nature of that threat and its devastating consequences, including the taking of innocent lives. Under the Convention scheme, it is properly for States to judge what systems are necessary for the protection of the general community from such threats.

3. It is of course acknowledged that the Convention scheme subjects those systems to ultimate European supervision. It does so because there are privacy interests in play. They are to be weighed against the need for the State to fulfil its paradigm, protective responsibility. The core purpose and fundamental aim of the Court's Article 8 jurisprudence has been and remains to ensure that the systems, operating as they must in secret, provide appropriate protection against abuse and arbitrariness by the

[1] For example, the plot to send suicide bombers onto 7 trains in Munich over Christmas 2015.

State. It is important that, in assessing the detail of appropriate protection, care is taken not to risk undermining the proper effectiveness of the systems for obtaining life-saving information and intelligence that cannot be obtained any other way. That is why the Court has consistently and rightly afforded States a broad margin of appreciation in determining whether measures that interfere with privacy are justified in the field of national security.

4. Some assert that the growth in the volume of internet traffic, and developments in technology, must necessitate a new legal approach or more safeguards. For example, it is suggested that no interception of any communications be undertaken at all, without reasonable suspicion in respect of the particular communication intercepted: an approach which would in practice (for reasons set out below) completely nullify the UK's ability to obtain intercept material from communications bearers. However, the scale of potential collection at the time that the Court previously considered bulk interception regimes in *Weber and Saravia v Germany*, app. 54934/00, ECHR 2006-XI ("*Weber*") and *Liberty v UK* app. 58243/00, 1 July 2008 ("*Liberty*") was already very considerable. Equally, traditional collection of traffic from communications satellites (undertaken by nearly every State) has inevitably always involved the interception of communications bearers carrying many hundreds of thousands if not millions of communications bundled together. There is no essential difference of kind between the UK's surveillance of communications obtained through interception of communications bearers, and the "strategic monitoring" addressed in *Weber*. The legal framework applied by the Court in *Weber* and *Liberty* has proved itself entirely adequate to control the use of interception by Council of Europe States.

5. By contrast, what has certainly changed is the sophistication of terrorists and criminals in communicating over the internet in ways that avoid detection, whether that be through the use of encryption, the adoption of bespoke communications systems, or simply the volume of internet traffic in which they can now hide their communications. The internet is now used widely both to recruit terrorists, and to direct terrorist attacks, as well as by cyber criminals. Imposing additional fetters on interception or intelligence sharing would damage Member States' ability to safeguard national security and combat serious crime, at exactly the point when

advances in communications technology have increased the threat from terrorists and criminals using the internet.

6. The UK has a detailed set of controls and safeguards in place governing the activities under challenge. The Intelligence Sharing Regime and the s.8(4) Regime are contained in a combination of primary legislation, published Codes and internal arrangements (which for good operational reasons cannot be made public). The detail is set out below (in **Section 2**). The bedrock of these Regimes are the Convention concepts of necessity and proportionality. These fundamental principles govern all aspects of information and intelligence from obtaining it in the first place, to examining it, to handling, storing and disclosing it, and finally to its retention and deletion. The safeguards built into the Regimes include a comprehensive and effective system of oversight by Parliamentary Committee (the Intelligence and Security Committee, "ISC"), a specially appointed Commissioner (a former Lord Justice of Appeal) and a specialist Tribunal, the Investigatory Powers Tribunal ("IPT"). As appears below, both the ISC and the Commissioner have examined the Regimes in detail and have publicly reported (see **§§1.19-1.35, §§2.26-2.41, §§2.105-2.124**). So too has the independent person appointed to keep terrorism laws under review, David Anderson QC. His report also contains useful material in the context of the present issues (see **§§1.21-1.35**).

7. The IPT is of particular importance in this case. That is because it conducted a conspicuously thorough and detailed examination of the very same issues that the Applicants now raise in the Liberty proceedings.[2] (see **§§1.41-1.51**) It sat as a tribunal of five distinguished lawyers, including two High Court Judges. It held open hearings, initially over 5 full days. It considered a very large quantity of evidence and submissions produced by the parties. The Applicants were represented throughout by experienced teams of Leading and Junior Counsel. It considered and applied the relevant Articles of the Convention (Articles 8, 10 and 14) and the Convention jurisprudence relating to them. It also conducted closed hearings. It did so because, unsurprisingly given the context, there were some relevant aspects (both relating to

[2] i.e. Proceedings in the IPT brought in 2013 by Liberty, Privacy, Amnesty International and various other civil liberties organisations, challenging the Intelligence Sharing and s.8(4) Regimes, in the same factual premises as are relevant to the present application. See the glossary.

the facts relating to the Applicants and relating to the nature of the safeguarding Regimes) which could not be considered in open without damaging national security. At those hearings, and more generally, the IPT was assisted by Leading Counsel acting as Counsel to the Tribunal. That assisted a thorough and rigorous examination of the relevant matters in closed – including specifically of the safeguards provided by internal arrangements in place to provide additional layers of protection surrounding any interferences with eg Article 8 rights. The IPT rightly concluded that the regimes were lawful and consistent with Articles 8, 10 and 14 ECHR[3].

8. In the Observations below, the Government begin by setting out some important points to be noted on the facts; and then the relevant domestic law and practice. The Government then addresses the questions posed by the Court in the following order below:

(1) ***Question 1:*** Whether in relation to the Intelligence Sharing Regime: (a) the Applicants can claim to be victims of violations of their rights under Article 8 ECHR; and (b) the acts of the UK are "in accordance with the law" and necessary within the meaning of Article 8 (**§§3.1-3.41**).

(2) ***Question 2:*** Whether in relation to the s.8(4) Regime: (a) the Applicants can claim to be victims of violations of their rights under Article 8 ECHR; and (b) the acts of the UK are "in accordance with the law" and necessary within the meaning of Article 8 (**§§4.1-4.108**).

(3) ***Question 3:*** The impact of the Applicants' status as NGOs on the Article 8 analysis (**§§5.1-5.4**).

(4) ***Question 4:*** Whether in relation to the s.8(4) Regime the acts of the United Kingdom are "prescribed by law" and necessary in a democratic society within the meaning of Article 10 ECHR (**§§6.1-6.39**).

(5) ***Question 5:*** Whether the proceedings before the IPT involved the determination of "civil rights and obligations" within the meaning of Art. 6(1). If so, whether the restrictions in the IPT proceedings taken as a whole were disproportionate or impaired the very essence of the applicants' right to

[3] In the case of the Intelligence Sharing Regime, that was with the benefit of further disclosure by the Intelligence Services of relevant internal safeguards during the proceedings, which was set out by the IPT in its judgments ("the Disclosure"), and which is now embodied in the Code.

a fair trial (**§§7.1-7.50**).

(6) ***Question 6:*** Whether there has been a violation of Article 14 taken together with Article 8 and/or Article 10 on account of the fact that the safeguards set out in s.16 of RIPA 2000 grants additional safeguards to people known to be in the British Islands? (**§§8.1-8.16**)

The facts and domestic law and practice

9. The Applicants' factual case both on the Intelligence Sharing and s.8(4) Regimes mischaracterises the nature of activities carried out under both regimes. In so doing, it reflects important misunderstandings perpetuated not just by commentators, but also by courts and other international bodies, which have repeated factual assumptions made without the benefit of input from the UK or US Governments, or understanding of the true position. The IPT, Commissioner and other independent UK bodies have confirmed this (as set out below). The Court should not proceed on the basis of such mischaracterisations. See further **§§1.1-1.28** below.

The Intelligence Sharing Regime

10. The Applicants' case challenges the UK's receipt of foreign intercept data collected by the US under the legal authority of s.702 Foreign Intelligence Surveillance Act 1978 ("FISA") (See Annex 2), pursuant to the "Prism" and "Upstream" programmes. The Applicants seriously mischaracterise the Prism and Upstream programmes. Neither Prism nor Upstream entails bulk interception by the US. Moreover, both programmes entail a detailed, recorded and audited process identifying particular selectors, such as phone numbers or email addresses, before interception can occur. In other words, they are targeted capabilities (see **§§1.1-1.18**). So far as the UK is concerned, it receives intelligence from the US and a range of other States. Before the IPT, Mr Charles Farr made a witness statement (See Annex 3) dealing with a range of factual matters and providing such explanations and descriptions of the Regimes as could be provided in open. As he explains, (a) receipt of foreign intelligence is vital to the protection of the public and provides intelligence not available from any other source and (b) it is not possible to distinguish between foreign intercept intelligence

and foreign intelligence derived in whole or in part from other sources (see **§§1.15-1.18**).

11. The detail of the domestic law and practice comprising the Intelligence Sharing Regime is set out in the body of the Observations (see **§§2.1-2.41**). As already noted, it comprises primary legislation based around the key Convention safeguards of necessity and proportionality - the SSA (See Annex 4) and the ISA (See Annex 5), as read with the CTA (See Annex 6); the HRA (See Annex 7); the DPA (See Annex 8); and the OSA (See Annex 9). That is supplemented by the Code (See Annex 10); and by internal arrangements (which are required to be made under the statutes governing each of the Intelligence Services). There is oversight by the ISC, the Commissioner and (as these cases demonstrate) the IPT.

The s.8(4) Regime

12. The Government can state (and has previously stated) that it intercepts communications in "bulk" – that is, at the level of communications cables – pursuant to the lawful authority of warrants under s.8(4) RIPA. Such interception is aimed at "external communications". It is described in general terms by the Commissioner in his Annual Reports of 2013 (See Annex 11) and 2014 (See Annex 12); in a report of the Intelligence and Security Committee of Parliament ("ISC") of 17 March 2015, *"Privacy and Security: A modern and transparent legal framework"* ("the ISC Report") at §§49-77 (See Annex 13); and in a report of the Investigatory Powers Review of June 2015 by David Anderson QC, *"A Question of Trust"* ("the Anderson Report") at chapter 10 (See Annex 14). All have been able to investigate the interception capabilities of the Intelligence Services in detail, with the full cooperation of the Services. Each has engaged with, or taken evidence from, many interested parties outside government, including some of the Applicants in this case, for the purposes of drafting their Reports. The Government can confirm the factual accuracy of the Reports' accounts of the Intelligence Services' capabilities (see **§§1.19-1.40**).

13. This ability and the manner in which it is operated is vital for the protection of national security. The s.8(4) Regime is critical to the discovery of threats and of targets who may be responsible for threats. That is particularly so given that, for

obvious reason, the Government does not have the same capabilities or intelligence opportunities in relation to external communications. The importance of the s.8(4) Regime is clear and has been acknowledged by the ISC, the Commissioner and David Anderson QC (see **§§1.29-1.35**). As the ISC put it: *"It is essential that the Agencies can "discover" unknown threats. This is not just about identifying individuals who are responsible for threats, it is about finding those threats in the first place. Targeted techniques only work on "known" threats: bulk techniques (which themselves involve a degree of filtering and targeting) are essential if the Agencies are to discover those threats"*: §77(K). David Anderson QC identified example case studies (see **§1.34**) which speak for themselves in terms of the importance of some of the intelligence derived from this Regime.

14. The s.8(4) Regime involves "bulk" interception. However, that is because that is the only practical way of obtaining access to the necessary data. Both resource and practical/technical issues dictate how the interception is done. The Commissioner's Annual Report of 2013 asked at §6.4.49 whether there were other reasonable but less intrusive means of obtaining needed external communications, and concluded at §6.5.51[4]: *"I am satisfied that at present there are no other reasonable means that would enable the interception agencies to have access to external communications which the Secretary of State judges it is necessary for them to obtain for a statutory purpose under the section 8(4) procedure. This is a sensitive matter of considerable technical complexity which I have investigated in detail."* (see **§1.33**)

15. Again, the Applicants significantly overstate their case. This is not, on any view, "mass surveillance". Nor is it "generalised access"; or targeting without suspicion. Any suggestion to the contrary is wrong. As is explained in more detail below, there are important limitations that lead to the position in which only the bearers which are most likely to yield valuable intelligence are even selected for interception. There is then a series of other selectors that limit and restrict the data subject to interception. And of that selection, only a small fraction is then ever selected for possible examination by an analyst. Such ultimate selection for examination is carefully controlled under the Regime, including specifically by reference to the concepts of necessity and proportionality. As the ISC correctly concluded at §77 of

[4] [***See Annex 11***]

its Report, the communications selected for examination *"are only the ones considered to be of the highest intelligence value. Only the communications of suspected criminals or national security targets are deliberately selected for examination."*(see **§§1.21-1.25**)

16. The true position is summarised by the Commissioner in his Annual Report for 2013 at §6.7.5:

> *"I am…personally quite clear that any member of the public who does not associate with potential terrorists or serious criminals or individuals who are involved in actions which could raise national security issues for the UK can be assured that none of the interception agencies which I inspect has the slightest interest in examining their emails, their phone or postal communications or their use of the internet, and they do not do so to any extent which could reasonably be regarded as significant."* (**§1.28**)

This is not, on any view, "mass surveillance". Nor is it "generalised access"; or targeting without suspicion.

17. So far as concerns domestic law and practice, the key legislation is RIPA. It contains a series of important and stringent safeguards. It is supplemented by the Code and by internal arrangements (see **§§2.42-2.104**). There is again oversight by the ISC, the Commissioner and the IPT – as described in detail below at **§§2.105-2.124**.

Article 8: the Intelligence Sharing Regime (Question 1)

Victim status

18. The Applicants are not "victims" for the purposes of Art. 34 ECHR, applying the principles in *Zakharov v Russia* app. 47143/06, 4 December 2015 (Grand Chamber). They do not belong to any group of persons possibly affected by the Intelligence Sharing Regime. They put forward no basis on which their communications are at realistic risk of being intercepted under the Prism or Upstream programmes, and shared with the Intelligence Services; and they do not assert that this has in fact happened (see **§§3.1-3.7**).

In accordance with the law[5]

19. The Intelligence Sharing Regime is in accordance with the law for the purposes of Article 8(2) ECHR. The statutory provisions in the Intelligence Sharing Regime provide domestic law powers (and the basis) for the obtaining and subsequent use of communications and communications data. Those provisions are clearly "accessible" (see **§3.10**).

20. The Intelligence Sharing Regime is also sufficiently "foreseeable" (see **§§3.11-3.21**). In this context, the essential test is whether the law indicates the scope of any discretion, and the manner of its exercise, with sufficient clarity to give the individual adequate protection against arbitrary interference: see §68 of *Malone v UK* (app. 8691/79), Series A no.82. The Grand Chamber has confirmed in *Zakharov* that this test remains the guiding principle when determining the foreseeability of intelligence-gathering powers (see §230). Further, this essential test must always be read subject to the important and well-established principle that the foreseeability requirement cannot mean that an individual should be enabled to foresee when the authorities are likely to resort to secret measures so that he can adapt his conduct accordingly: *Malone* at §67; *Leander v. Sweden*, 26 March 1987, Series A no.116, at §51; and *Weber* at §93. The Intelligence Sharing Regime satisfies this test.

21. **First**, the regime is sufficiently clear as regards the circumstances in which the Intelligence Services can in principle **obtain** information from the US authorities, which has been gathered under the Prism or Upstream programmes (see **§§3.11-3.16**). The purposes for which such information can be obtained are explicitly set out in ss.1-2 SSA, and ss.1-2 and 3-4 ISA, which set out the functions of the Intelligence Services. They are the interests of national security, in the context of the various Intelligence Services' particular functions; the interests of the economic wellbeing of the United Kingdom; and the prevention and detection of serious crime. Moreover, the circumstances in which the Intelligence Services may obtain information under the Intelligence Sharing Regime are further defined and circumscribed by the Code and Disclosure (which reflect what has always been the practice of the Intelligence

[5] No separate issue arises as to 'necessity' of the Intelligence Sharing Regime, and no submissions are made about it by the Applicants.

Services). In particular, the Code provides a series of detailed public safeguards on obtaining information.

22. **Secondly**, the Intelligence Sharing Regime is similarly sufficiently clear as regards the subsequent handling, use and possible onward disclosure of communications and communications data obtained by the Intelligence Services (see **§§3.17-3.21**). Handling and use is addressed by (i) s. 19(2) of the CTA, as read with the statutory definitions of the Intelligence Services' functions (in s. 1 of the SSA and ss. 1 and 3 of ISA); (ii) the general proportionality constraints imposed by s. 6 of the HRA and - as regards retention periods in particular - the fifth data protection principle; and (iii) the seventh data protection principle (as reinforced by the criminal offence in ss. 1(1) and 8(1) of the OSA) as regards security measures whilst the information is being stored. Further, ss. 1-2 of the SSA and ss. 1-2 and 3-4 of the ISA, as read with ss. 19(3)-(5) of the CTA and s. 6(1) of the HRA, sufficiently address the circumstances in which the Intelligence Services may disclose information obtained from a foreign intelligence agency to others. In addition, disclosure in breach of the "arrangements" for which provision is made in s. 2(2)(a) of the SSA and ss. 2(2)(a) and 4(2)(a) of the ISA is rendered criminal by s. 1(1) of the OSA. Moreover, additional safeguards as to the handling, use and onward disclosure of material obtained under the Intelligence Sharing Regime are provided by the Code. Specifically, chapter 12 of the Code provides that where the Intelligence Services receive intercepted communications content or data from a foreign state, irrespective whether it is solicited or unsolicited, analysed or unanalysed, and whether or not the communications data is associated with the content of communications, the communications content and data are subject to exactly the same internal rules and safeguards as the same categories of content or data, when the material is obtained directly by the Intelligence Services as a result of interception under RIPA.

23. **Thirdly**, when considering whether the Intelligence Sharing Regime is "*foreseeable*", the Court should take into account the available oversight mechanisms – namely, the ISC, the IPT, and (as set out above, with respect to oversight of the relevant internal "arrangements" themselves) the Commissioner (see **§§3.22-3.27**). The relevance of oversight mechanisms in the assessment of foreseeability, and in particular the existence of adequate safeguards against abuse, is well established in the Court's

case law: see e.g. *Kennedy*: when considering the general ECHR-compatibility of the RIPA s. 8(1) regime, the Court at §§155-170 of *Kennedy* "*jointly*" considered the "*in accordance with the law*" and "*necessity*" requirements, and in particular analysed the available oversight mechanisms (at §§165-168) in tandem with considering the foreseeability of various elements of the regime (§§156-164). See too the Grand Chamber's judgment in *Zakharov*, where the Court examined *"with particular attention"* the supervision arrangements provided by Russian law, as part of its assessment of the existence of adequate safeguards against abuse: §§271-280.

24. **Finally**, having regard to the core purpose of the in accordance with the law requirement as identified eg in *Malone,* it is important to note that the IPT has examined the Intelligence Services' internal safeguards in the context of the Intelligence Sharing Regime in detail, and has found that adequate internal safeguards exist[6], and that the Regime as a whole (with the benefit of the Disclosure, now mirrored in the Code) is in accordance with the law (see **§3.28**). The applicable internal safeguards have now been examined not just by the Commissioner, but also by the domestic courts, and have been found to offer an important strand of protection for the purposes of rights under the Convention.

25. These were the conclusions of the IPT after its careful examination of the issues (see **§1.45**). It is submitted that there is no reason for the Court to reach any different view.

The s.8(4) regime (Question 2)

Victim status

26. As is the case in respect of the Intelligence Sharing Regime (see §18 above), the Applicants are not "victims" applying the principles in *Zakharov* (save for the two

[6] See §55 of the IPT's 5 December Judgment: *"Having considered the arrangements below the waterline, as described in the judgment, we are satisfied that there are adequate arrangements in place for the purpose of ensuring compliance with the statutory framework and with Articles 8 and 10 of the Convention, so far as the receipt of intercept from Prism and/or Upstream is concerned." (See Annex 15)*

organisations who received a declaration in the IPT proceedings[7]). The Applicants cannot demonstrate that they are at realistic risk of selection/examination under the s.8(4) Regime i.e. that they have reason to believe their communications are of interest to the Intelligence Services on the grounds mentioned in s.5(3)(a), (b) or (c) (in the interests of national security, for the purposes of preventing or detecting serious crime or for the purpose of safeguarding the economic well-being of the United Kingdom) (see §4.1 below).

Lawfulness of the s.8(4) Regime

27. There is no good reason for the ECtHR to reach any different conclusion than it reached on the lawfulness of the parallel regime for the interception of communications under s.8(1) RIPA in *Kennedy v UK* (app. 26839/05, 18 May 2010). The IPT has also examined the issue of the lawfulness of the s.8(4) Regime with conspicuous care; and it is submitted reached the correct conclusion that the Regime was in accordance with law applying the Court's jurisprudence (**§§1.46-1.47**). The s.8(4) Regime satisfies the "in accordance with the law" and "necessity" tests.

In accordance with the law

28. The statutory provisions of RIPA provide domestic law powers for the regime. The "accessibility" requirement is satisfied in that RIPA is primary legislation and the Code is a public document, and insofar as the operation of the s. 8(4) Regime is further clarified by the Commissioner's Reports, those are also public documents (**§4.32**).

29. As to foreseeability, the ECtHR has set out at §95 of *Weber and Saravia v Germany,* (dec.), app. 54934/00, ECHR 2006-XI ("*Weber*") the six "minimum safeguards" that the domestic legal framework needs to set out in the context of the interception of communications ("the *Weber* criteria") (see **§4.35**). *"[1] the nature of the offences which may give rise to an interception order; [2] a definition of the categories of people liable to have their telephones tapped; [3] a limit on the duration of telephone tapping; [4] the procedure to be followed for examining, using and storing the data obtained; [5] the precautions to be taken*

[7] i.e. Amnesty International and the Legal Resources Centre – see §1.50 and §§4.100-4.108 below.

when communicating the data to other parties; and [6] the circumstances in which recordings may or must be erased or the tapes destroyed ..." (*Weber*, at §95). Each of the *Weber* criteria is satisfied by the Regime **(see §§4.40-4.55 below)**. See also *Kennedy* at §§155-167.

30. In relation to interception of the content of communications:

***(1) The "offences" which may give rise to an interception order*:** This requirement is satisfied by s. 5 of RIPA, as read with the relevant definitions in s.81 of RIPA and §§6.11-6.12 of the Code. This follows, in particular, from a straightforward application of §159 of *Kennedy*, and §133 of *RE v United Kingdom* (see **§4.40** and see further below at **§§3.13-3.15** and **§§4.77-4.81** as regards the meaning of "national security").

***(2) The categories of people liable to have their 'telephones tapped'*:**
As is clear from §97 of *Weber*, this second requirement in §95 of *Weber* applies both to the interception stage (which merely results in the obtaining / recording of communications) and to the subsequent selection stage (which results in a smaller volume of intercepted material being read, looked at or listened to by one or more persons) (see **§4.41**).

As regards the *interception* stage (see **§4.42**):

(1) As appears from s. 8(4)(a) and s. 8(5) of RIPA, a s. 8(4) warrant is directed primarily at the interception of external communications.

(2) The term "communication" is sufficiently defined in s. 81 of RIPA. The term "external communication" is sufficiently defined in s. 20 and §5.1 of the Code (see **§§4.66-4.76** below). The s. 8(4) regime does not impose any limit on the types of "external communications" at issue, with the result that the broad definition of "communication" in s. 81 applies in full and, in principle, anything that falls within that definition may fall within s. 8(5)(a) insofar as it is "external".

(3) Further, the s. 8(4) regime does not impose any express limit on number of external communications which may fall within "the description of communications to which the warrant relates" in s. 8(4)(a). As is made clear in numerous public documents, a s. 8(4) warrant may in principle result in

the interception of "substantial quantities of communications…contained in "bearers" carrying communications to many countries"[8]. Similarly, during the Parliamentary debate on the Bill that was to become RIPA, Lord Bassam referred to intercepting the whole of a communications "link".

(4) In addition, a s. 8(4) warrant may in principle authorise the interception of internal communications insofar as that is necessary in order to intercept the external communications to which the s. 8(4) warrant relates. See s. 5(6) of RIPA, and the reference back to s. 5(6) in s. 8(5)(b) of RIPA (which latter provision needs to be read with s. 8(4)(a) of RIPA). This point was also made clear to Parliament and it has in any event been publicly confirmed by the Commissioner.

(5) In the circumstances, and given that an individual should not be enabled "*to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly*" and in the light of the available oversight mechanisms, the s. 8(4) regime sufficiently identifies the categories of people who are liable to have their communications intercepted.

As regards the *selection* stage (see **§4.43**):

(1) No intercepted material (whether external or not) will be read, looked at or listened to by any person unless it falls within the terms of the Secretary of State's certificate, and unless (given s. 6(1) HRA) it is proportionate to do so in the particular circumstances of the case.

(2) As regards the former, material will only fall within the terms of the certificate insofar as it is of a category described therein; and insofar as the examination of it is necessary on the grounds in s. 5(3)(a)-(c) RIPA. Those grounds are themselves sufficiently defined for the purposes of the foreseeability requirement: see §159-160 of *Kennedy*.

(3) Further, s. 16(2) RIPA, as read with the exceptions in s. 16(3)-(5A), place sufficiently precise limits on the extent to which intercepted material can be selected to be read, looked at or listened to according to a factor which is (a) referable to an individual who is known to be for the time being in the British Islands and (b) which has as its purpose, or one of its purposes, the identification of material contained in communications sent by him or

[8] See the 5 December Judgment at §93. See too, for example, the ISC Report.

intended for him.

(3) Limits on the duration of 'telephone tapping': The s. 8(4) Regime makes sufficient provision for the duration of any s.8(4) warrant, and for the circumstances in which such a warrant may be renewed: see **§§4.49-4.50** below, §161 of *Kennedy,* and the specific provisions for renewal of a warrant contained in §§6.22-6.24 of the Code[9].

***(4)-(5) The procedure to be followed for examining, using and storing the data obtained; and the precautions to be taken when communicating the data to other parties*: (see §§4.51-4.53)**

Insofar as the intercepted material cannot be read, looked at or listened to by a person pursuant to s.16 (and the certificate in question), it is clear that it cannot be used at all. Prior to its destruction, it must of course be securely stored (§7.7 of the Code).

As regards the intercepted material that can be read, looked at or listened to pursuant to s.16 (and the certificate in question), the applicable regime is well sufficient to satisfy the fourth and fifth foreseeability requirement in §95 of *Weber*. See §163 of *Kennedy*, and the following matters (various of which add to the safeguards considered in *Kennedy*):

(1) Material must generally be selected for possible examination, applying search terms, by equipment operating automatically for that purpose (so that the possibility of human error or deliberate contravention of the conditions for access at this point is minimised). Moreover, before any material can be examined at all, the person examining it must create a record setting out why access to the material is required and proportionate, and consistent with the applicable certificate, and stating any circumstances that are likely to give rise to a degree of collateral infringement of privacy, and any measures taken to

[9] Note too that the provisions for renewal of a warrant contained in §§6.22-6.24 of the Code are at least as detailed as those found lawful by the ECtHR in relation to the renewal of warrants for covert surveillance under Part II RIPA, considered in *RE v United Kingdom*: see *RE* at §137. Contrast §162 of the Application, which wrongly states that chapter 6 of the Code does not *"impose any limits on the scope or duration of warrants".*

reduce the extent of that intrusion. See Code, §§7.14-7.16.

(2) The Code affords further protections to material examined under the s.8(4) Regime at §§7.11-7.20. Thus, material should only be examined by authorised persons receiving regular training in the operation of s.16 RIPA and the requirements of necessity and proportionality; systems should to the extent possible prevent access to material without the record required by §7.16 of the Code having been created; the record must be retained for the purposes of subsequent audit; access to the material must be limited to a defined period of time; if access is renewed, the record must be updated with the reasons for renewal; systems must ensure that if a request for renewal of access is not made within the defined period, no further access will be granted; and regular audits, including checks of the particular matters set out in the Code, should be carried out to ensure that the requirements in s.16 RIPA are met.

(3) Material can be used by the Intelligence Services only in accordance with s. 19(2) of the CTA, as read with the statutory definition of the Intelligence Services' functions (in s. 1 of the SSA and ss. 1 and 3 of the ISA) and only insofar as that is proportionate under s. 6(1) of the HRA. See also §7.6 of the Code as regards copying and §7.7 of the Code as regards storage (the latter being reinforced by the seventh data protection principle).

(4) Further, s. 15(2) sets out the precautions to be taken when communicating intercepted material that can be read, looked at or listened to pursuant to s. 16 to other persons (including foreign intelligence agencies: see §3.109 above). These precautions serve to ensure *e.g.* that only so much of any intercepted material or related communications data as is "*necessary*" for the authorised purposes (as defined in s. 15(4)) is disclosed. The s. 15 safeguards are supplemented in this regard by §§7.4 and 7.5 of the Code. In addition, any such disclosure must satisfy the constraints imposed by ss. 1-2 of the SSA and ss. 1-2 and 3-4 of the ISA, as read with ss. 19(3)-(5) of the CTA and s. 6(1) of the HRA. Further, and as in the case of the Intelligence Sharing and Handling Regime, disclosure in breach of the "arrangements" for which provision is made in s. 2(2)(a) of the SSA and ss. 2(2)(a) and 4(2)(a) of the ISA is rendered criminal by s. 1(1) of the OSA.

(5) The detail of the s. 15 and s.16 arrangements is kept under review by the Commissioner (see §§2.79-2.81 and 2.97-2.98 below).

(6) The circumstances in which recordings may or must be erased or the tapes destroyed **(see §§4.54-4.55)**

Section 15(3) of RIPA and §§7.8-7.9 of the Code (including the obligation to review retention at appropriate intervals, and the specification of maximum retention periods for different categories of material, which should normally be no longer than 2 years) make sufficient provision for this purpose. See *Kennedy* at §§164-165 (and note that further safeguards in §7.9 of the Code, including the specification of maximum retention periods, have been added to the Code since *Kennedy*). Both s. 15(3) and the Code are reinforced by the fifth data protection principle.

31. The acquisition of **communications data** has rightly been considered by the ECtHR to be less intrusive in Art. 8 terms than the covert acquisition of the content of communications, and that remains true in the internet age (see **§§4.29-4.31**). For that reason, the *Weber* criteria do not apply to the acquisition of communications data (and have never been held by the ECtHR so to apply). The applicable test is simply whether the law gives the individual adequate protection against arbitrary interference. The s.8(4) Regime satisfies that test. In any event if, contrary to the above, the *Weber* criteria apply to communications data, they are met (see **§§4.60-4.61**)

(1) As a preliminary point, the controls within the s.8(4) Regime for "related communications data" - as opposed to content - apply to only a limited subset of metadata. "Related communications data" for the purposes of the s.8(4) Regime has the statutory meaning given to it by ss.20 and 21 RIPA. That meaning is not synonymous with, and is significantly narrower than, the term "metadata", used by the Applicants in this context. The Applicants define "metadata" as "*structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource*" (see Application, §21). On that definition, much "metadata" amounts to the content of communications for the purposes of the s.8(4) Regime, not related communications data (since all information that is not "related communications data" must be treated as content). For instance, if a processing system was able to extract or generate a structured index of the

contents of a communication, it would be "metadata"; but would be content for the purposes of the s.8(4) Regime. Extracting email addresses or telephone numbers from the body of a communication would generate "metadata"; but would be "content" for the purposes of the s.8(4) Regime. The language or format used for a communication would be "metadata"; but again, "content" for the purposes of the s.8(4) Regime.

(2) The s. 8(4) Regime is sufficiently clear as regards the circumstances in which the Intelligence Services can **obtain** related communications data: see **§§4.41-4.43** below, which applies equally here.

(3) Once obtained, **access** to any related communications data must be necessary and proportionate under s. 6(1) of the HRA, and will be subject to the constraints in ss.1-2 of the SSA and ss. 1-2 and 3-4 of the ISA. Any access by any foreign intelligence partner at this stage would be constrained by ss. 15(2)(a) and 15(2)(b) of RIPA (as read with s. 15(4)); and, as it would amount to a disclosure by the Intelligence Service in question to another person would similarly have to comply with s. 6(1) of the HRA and be subject to the constraints in ss. 1-2 of the SSA and ss. 1-2 and 3-4 of the ISA, as read with ss. 19(3)-(5) of the CTA.

(4) Given the constraints in ss. 15 of RIPA and s. 6(1) of the HRA, communications data cannot be used (in combination with other information / intelligence) to discover *e.g.* that a woman of no intelligence interest may be planning an abortion. This is for the simple reason that obtaining this information would very obviously serve none of the authorised purposes in s. 15(4), and would not be in pursuance of any of the Intelligence Services' statutory functions. There is nothing unique about communications data (even when aggregated) here.

(5) Further, there is good reason for s. 16 of RIPA covering access to intercepted material (*i.e.* the content of communications) and not covering access to communications data (see the Applicants' complaints at §46(1) of their Additional Submissions). In order for s. 16 to work as a safeguard in relation

to individuals who are within the British Islands, but whose communications might be intercepted as part of the S. 8(4) Regime, the Intelligence Services need information to be able to assess whether any potential target is "*for the time being in the British Islands*" (for the purposes of s. 16(2)(a)). Communications data is a significant resource in this regard. In other words, an important reason why the Intelligence Services need access to related communications data under the s. 8(4) Regime is precisely so as to ensure that the s. 16 safeguard works properly and, insofar as possible, factors are not used at the selection stage that are - albeit not to the knowledge of the Intelligence Services - "*referable to an individual who is ... for the time being in the British Islands*".

(6) The regime equally contains sufficient clear provision regarding the subsequent handling, use and possible onward disclosure by the Intelligence Services of related communications data.

32. None of the principal criticisms of the regime made by the Applicants (the scope of "external communications", the meaning of "national security", and the fact that warrants are not issued by judges) is well-founded, or prevents the Regime being "in accordance with the law". The concepts of "external communications" and "national security" are properly used and sufficiently precise: see **§§3.13-3.15, §§4.77-4.81 and §§4.42, §§4.66-4.76** below. As to the contention that prior judicial authorisation is necessary (see **§§4.96-4.99**):

(1) The Government strongly deny that the Convention requires or should require any such precondition. Just as in *Kennedy*, the extensive oversight mechanisms in the s.8(4) Regime offer sufficient safeguards to render the regime in accordance with the law, without any requirement for independent (still less, judicial) **pre-**authorisation of warrants.

(2) The Court's case law does not require independent authorisation of warrants as a precondition of lawfulness, provided that the applicable regime otherwise contains sufficient safeguards. It is on the whole in principle desirable to entrust *supervisory* control to a judge: but such control may consist of *oversight* after rather

than before the event: see *Klass v Germany*, 6 September 1978, Series A no.28 at §51, *Kennedy* at §167, and most recently, the detailed consideration of the issue in *Szabo and Vissy v Hungary* app.37138/14 (12 January 2016) at §77:

"The Court recalls that in Dumitru Popescu (cited above, §§70-73) it expressed the view that either the body issuing authorisations for interception should be independent or there should be control by a judge or an independent body over the issuing body's activity. Accordingly, in this field, control by an independent body, normally a judge with special expertise, should be the rule and substitute solutions the exception, warranting close scrutiny (see Klass and others, cited above, §§42 and 55). The ex ante authorisation of such a measure is not an absolute requirement per se, because where there is extensive post factum judicial oversight, this may counterbalance the shortcomings of the authorisation (see Kennedy, cited above, §167)." (Emphasis added)

(To the extent that *Iordachi v Moldova* app.25198/02, 10 February 2009 implies at §40 that there must in all cases be independent prior authorisation of warrants for interception, it is inconsistent with the later cases of *Kennedy* and *Szabo*, and cannot stand with the general thrust of the Court's case law.)

(3) There is extensive independent (including judicial) *post factum* oversight of secret surveillance under the s.8(4) Regime. The very same observations made by the ECtHR at §167 of *Kennedy*, in which the Court found that the oversight of the IPT compensated for the lack of prior authorisation, apply equally here:

"…the Court highlights the extensive jurisdiction of the IPT to examine any complaint of unlawful interception. Unlike in many other domestic systems, any person who suspects that his communications have been or are being intercepted may apply to the IPT. The jurisdiction of the IPT does not, therefore, depend on notification to the interception subject that there has been an interception of his communications. The Court emphasises that the IPT is an independent and impartial body, which has adopted its own rules of procedure. The members of the tribunal must hold or have held high judicial office or be experienced lawyers. In undertaking its examination of complaints by individuals, the IPT has access to closed material and has the power to require the Commissioner to provide it with any assistance it thinks fit and the power to order disclosure by those involved in the

authorisation and execution of the warrant of all documents it considers relevant. In the event that the IPT finds in the applicant's favour, it can, inter alia, quash any interception order, require destruction of intercept material and order compensation to be paid. The publication of the IPT's legal rulings further enhances the level of scrutiny afforded to secret surveillance activities in the United Kingdom."

(4) Moreover, the following additional points about the applicable *post factum* independent oversight should also be made. The IPT is not only in principle but in fact an effective system of oversight in this type of case, as the Liberty proceedings indicate. The Commissioner oversees the issue of warrants under the s.8(4) Regime as part of his functions, and looks at a substantial proportion of all individual warrant applications in detail. The extent of his post factum oversight is illustrated (for example) by the detail of his 2013 Annual Report, which specifically addressed issues raised in this Application. The ISC also provides an important means of overseeing the s.8(4) Regime as a whole, and specifically investigated the issuing of warrants in the ISC Report (see the report, pp.37-38, [See Annex 13]).

(5) Finally, the Applicants seek to place reliance on the CJEU judgment in *Digital Rights Ireland (See Annex 16)*. That case did not on any view purport to lay down minimum procedural safeguards under EU law. Nor did it purport to alter, expand or develop Convention jurisprudence (on the contrary, it referred to and purported to apply that jurisprudence – although it is notable that it simply did not consider or apply much of the relevant Convention jurisprudence). The CJEU has in any event been invited to consider the issues again following the reference made to it by the English Court of Appeal in *R (Davis and Watson) v Secretary of State for the Home Department* (see **§§4.17-4.28**) (See Annex 17)

Necessity

33. The s.8(4) Regime clearly satisfies the "necessity" test, not least given the State's margin of appreciation in this area (see **§§4.84-4.95**). It is subject to sufficient safeguards against abuse (for all the reasons already given with regard to the "in accordance with the law" test). It is also essential if the Intelligence Services are both

to discover and to address national security threats effectively. As the findings in the ISC and Anderson Reports indicate, it has enabled the discovery and successful disruption of major threats, in circumstances where interception under the regime was the only means likely to produce the necessary intelligence. It would be absurd if the case law of the ECtHR required a finding of disproportionality in such circumstances, merely because the whole contents of a bearer are intercepted, even though only a tiny fraction of intercepted communications are ever, and can ever be, selected for potential examination, let alone examined. On a proper analysis, it does not.

Article 10 and NGO's (Questions 3 and 4)

34. The potential for confidential NGO material to be intercepted in the course of the operation of the s.8(4) Regime does not affect the correctness of the analysis summarised above (see **§§5.1-5.4**). Nor does the engagement of Article 10 in respect of such material give rise to a requirement for additional safeguards beyond those required by Article 8 (see **§§6.1-6.39**). The cases to which the Court has referred in its question – *Nordisk Film*[10], *Financial Times Ltd*[11], *Telegraaf Media* and *Nagla* – are all cases concerned with targeted measures directed to the identification and/or disclosure of journalistic sources. None of them is concerned with strategic monitoring of the type conducted under the s.8(4) Regime. In particular, there is no requirement for prior judicial authorisation in respect of the interception of NGO material under the s.8(4) Regime.

Article 6 (Question 5)

35. The domestic IPT proceedings in *Liberty* did not involve the determination of "civil rights and obligations" within the meaning of Article 6(1). There is a clear and consistent line of ECtHR authority which makes clear that the rights at issue in the field of secret interception powers are not "civil" rights (see **§§7.1-7.10**). In the alternative, even if Art. 6 did apply to the proceedings before the IPT, it was satisfied.

[10] *Nordisk Film & TV A/S v Denmark* App. No. 40485/02, 8 December 2005.
[11] *Financial Times Ltd and Others v the United Kingdom*, App. No. 821/03, 15 December 2009; (2010) 50 EHRR 1153.

Looked at as a whole, the IPT's procedures plainly did not impair the very essence of the applicants' right to a fair trial, particularly given the Court's conclusions in *Kennedy v United Kingdom* (see **§§7.11-7.50**) .

Article 14 (with Articles 8 and/or 10)

36. As to the assertion that the s.8(4) regime is indirectly discriminatory on grounds of nationality contrary to Article 14 ECHR (see **§§8.1-8.16**):

(1) The operation of the s.8(4) Regime does not mean that persons outside the United Kingdom are disproportionately likely to have their private communications intercepted. The Applicants' case is factually incorrect.

(2) At the stage when communications are selected for examination, the s.8(4) Regime provides an additional safeguard for persons known to be within the British Islands. The Secretary of State must certify that it is necessary to examine intercepted material by reference to a factor referable to such a person. To that extent, persons are treated differently on the basis of current location.

(3) However, the application of that safeguard to persons known to be within the British Islands, and not to persons outwith the British Islands, does not constitute a relevant difference in treatment for the purposes of Article 14 ECHR.

(4) Moreover, even if it did constitute a relevant difference in treatment for the purposes of Article 14, it would plainly be justified.

1 PART I - THE FACTS

1.1 The intelligence gathering activities and capacities of the UK, and the nature of interception programmes in the UK and US, have been widely mischaracterised as a result of the Snowden allegations. A number of mischaracterisations and inaccuracies have found their way into court judgments in proceedings to which neither the UK nor US governments were parties, or into texts of international institutions into which neither the UK nor US governments have had input. There, they have been presented as established fact, when they are anything but. Those errors are repeated by the Applicants and Intervenors in this case.

1.2 The difficulty of addressing such errors is compounded because it has been the policy of successive UK Governments to neither confirm nor deny ("NCND") assertions, allegations or speculation in relation to the Intelligence Services. By its very nature, the work of the Intelligence Services provides the paradigm example of a context where secrecy is required if the work is to be effective, and there is an obvious, and widely recognised, need to preserve that effectiveness. This means, as a general rule, the Government will adopt a position of NCND when addressing the Services' precise activities and capabilities. So it is only possible to address mischaracterisations in open to a limited extent.

1.3 That having been said, there are reports in which the activities and capabilities of the Intelligence Services are addressed, where the authors have taken evidence from the Intelligence Services, and which the Government can confirm are factually accurate. Those are a report of the Intelligence and Security Committee of Parliament ("ISC") of 17 March 2015[12], *"Privacy and Security: A modern and transparent legal framework"* ("the ISC Report"); a report of the Investigatory Powers Review of June 2015 by David Anderson QC, *"A Question of Trust"* ("the Anderson Report")[13]; and the regular annual (and now, twice-yearly) reports of the Commissioner. The US position as regards Prism and Upstream has also been set out by the US Executive Branch itself in various documents, as detailed below. The Court can rely upon those

[12] See [***Annex 13***]
[13] See [***Annex 14***]

sources. But otherwise, the Court cannot assume the truth of any of the broad factual assertions made in the Application, or indeed in submissions from the Intervenors, save where consistent with those Reports, and/or with material from the US Executive Branch; and it should not do so.

1.4 The most significant material factual errors asserted in the Application are addressed either in the "facts" section below, or in the body of the response to the Applicants' grounds, to the extent that the NCND principle allows them to be addressed. Separate and additional errors made by Intervenors will be addressed in the response to the interventions.

(1) The Prism/Upstream complaint

The Prism and Upstream programmes

1.5 The Applicants' case[14] challenges the UK's receipt of foreign intercept data collected by the US under the legal authority of s.702 Foreign Intelligence Surveillance Act 1978 ("FISA"), pursuant to the "Prism" and "Upstream" programmes. It is unnecessary for the Court to make detailed factual findings about the nature of the Prism and Upstream programmes, even if it were appropriate to do so, since the Applicants' case does not depend upon the precise nature of those programmes. However, it is important to observe that the consistent characterisation of these programmes as concerning "mass communications surveillance", both in the Application and in various submissions from interveners in this case, is simply wrong. The Applicants' broad characterisation of the nature of those programmes is flatly contradicted in a number of important respects by publicly available material, including from the US Government itself. No assumption can or should be made as to the truth of any of the Applicants' assertions, save where they are consistent with the US Government's own factual explanation.

1.6 By way of example, the Applicants assert that under Prism and Upstream, the two programmes provide for the *"bulk"* collection of *"vast amounts of communications and communications data carried by the submarine fibre optic cables passing through, into and*

[14] See "Additional Submissions on Facts and Complaints" at §§70-73.

out of the US" and that they are *"designed to capture the private communications of individuals across the globe"*: see Application Form Statement of Facts p4. This is wholly contrary to material from the US Government, contained in (i) a report of 18 April 2014 of the NSA Director of Civil Liberties and Privacy Office, *"NSA's Implementation of Foreign Intelligence Surveillance Act Section 702"*[15]; (ii) a paper from the Director of National Intelligence of 8 June 2013, *"Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act"*[16]; and (iii) a paper of 9 August 2013 from the NSA, *"The National Security Agency: Missions, Authorities, Oversight and Partnerships"*[17]. On the basis of that material, the position is rather that:

(1) The NSA's collection authorities stem from two key sources: Executive Order 12333 and FISA. All collection under any authority must be undertaken for foreign intelligence and counterintelligence purposes. Prism and Upstream are undertaken under the authority of FISA.

(2) Both Prism and Upstream require an NSA analyst to identify a specific non-US person located outside the US (e.g. a person belonging to a foreign terrorist organisation) as a "target", and to obtain a unique identifier associated with that target, such as an email address, to be used as a tasked "*selector*".

(3) The analyst must verify the connection between the target and the selector, and must document (a) the foreign intelligence information expected to be acquired; and (b) the information that would lead a reasonable person to conclude that the selector was associated with a non-US person outside the US. That documentation must be reviewed and approved or denied by two independent processes.

(4) Under Prism, service providers are compelled to provide the NSA with communications to or from such approved selectors. Under Upstream, service providers are required to assist the NSA lawfully to intercept communications to, from, or about approved selectors.

[15] See [***Annex 18***]
[16] See [***Annex 19***]
[17] See [***Annex 20***]

(5) Thus, neither Prism nor Upstream entails bulk interception. Moreover, both programmes entail a detailed, recorded and audited process identifying particular selectors, such as phone numbers or email addresses, before interception can occur[18].

(6) Both programmes are undertaken with the knowledge of the service provider, and under procedures approved by the FISA Court. All information obtained is based upon a written directive from the Attorney General and the Director of National Intelligence, detailing the foreign intelligence categories within which access requests must fall. Any such written directive is reviewed annually by the FISA Court.

(7) The NSA has a compliance programme, designed to ensure that its activities are conducted in accordance with law and procedure; therefore, in the case of Prism and Upstream, in accordance with s.702 FISA and associated requirements. Issues of non-compliance must be reported to the Office of the Director of National Intelligence and the Department of Justice for further reporting to the FISA Court and Congress, as required. ODNI and DOJ also regularly do audits of the NSA's compliance with targeting and minimisation procedures, including reviewing selectors used by the NSA.

1.7 The mischaracterisation of Prism and Upstream as involving "*bulk seizure, acquisition, collection and storage*" appears to result from a failure to distinguish between two different types of NSA programme. The NSA has indeed operated a programme which involved the collection of telephone call records, including the records of US citizens (but not the content of telephone conversations) in bulk. However, that programme was not Prism or Upstream. It was an entirely different programme, approved by the Foreign Intelligence Surveillance Court ("FISC") pursuant to section 215 of the USA Patriot Act (that section being replicated in FISA as section 501) ("the Section 215 Programme"). The US Privacy and Civil Liberties Oversight Board ("PCLOB"), an independent, bipartisan agency within the US government's executive branch, was tasked with investigating both the Section 215 Programme and collection under the authority of s.702 FISA (i.e. Prism/Upstream) in July 2013, following the Snowden allegations. In January 2014, it recommended that the Section

[18] See too the ISC's 17 July 2013 Statement at §4 (***See Annex 21***): *"Access under Prism is specific and targeted (not a broad "data mining" capability, as has been alleged)*".

215 Programme should end. The programme was subsequently ended by the USA Freedom Act, which was enacted in June 2015, and came into force on 29 November 2015 (See Annex 22).

1.8 PCLOB reached very different conclusions regarding Prism and Upstream. Its investigation of Prism and Upstream is substantially contained in a report of 2 July 2014, *"Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act"* ("PCLOB's 2 July Report"[19]). The Report summarised the nature of Prism and Upstream as follows at p.111, in terms which are entirely consistent with the position set out above:

> *"Unlike the telephone records program conducted by the NSA under Section 215 of the USA Patriot Act, the Section 702 program[20] is not based on the indiscriminate collection of information in bulk. Instead, the program consists entirely of targeting specific persons about whom an individualised determination has been made. Once the government concludes that a specific non-U.S. person located outside the United States is likely to communicate certain types of foreign intelligence information – and that this person uses a particular communications "selector", such as an email address or telephone number – the government acquires only those communications involving that particular selector.*
>
> *Every individual decision to target a particular person and acquire the communications associated with that person must be documented and approved by senior analysts within the NSA before targeting. Each targeting decision is later reviewed by an oversight team from the DOJ[21] and the ODNI[22] ("the DOJ/ODNI oversight team") in an effort to ensure that the person targeted is reasonably believed to be a non-US person located abroad, and that the targeting has a legitimate foreign intelligence purpose. The FISA Court does not approve individual targeting decisions or review them after they are made."*

1.9 PCLOB made 10 policy recommendations concerning the s.702 programme, in order to ensure protection of privacy rights. All of those recommendations have now been implemented in full or in part (see PCLOB's *"Recommendations Assessment Report"* of

[19] See [***Annex 23***]
[20] The "Section 702 program" includes both Prism and Upstream.
[21] The US Department of Justice
[22] The Office of the Director of National Intelligence

5 February 2016[23]). However, PCLOB's overall conclusion was that the s.702 programme (incorporating Prism/Upstream) was a lawful and valuable resource, consistent with US privacy rights under the Fourth Amendment. See e.g. p.9 of the 2 July Report:

> *"The Board also concludes that the core of the Section 702 program – acquiring the communications of specifically targeted foreign persons who are located outside the United States, upon a belief that those persons are likely to communication foreign intelligence, using specific communications identifiers, subject to FISA court-approved targeting rules and multiple layers of oversight – fits with the "totality of the circumstances" standard for reasonableness under the Fourth Amendment[24], as that standard has been defined by courts to date."*

1.10 The Government recognises that the Applicants' misunderstanding of the effect of the Prism and Upstream programmes is widely shared, and has been repeated by various courts or other bodies in Council of Europe States[25]. Nevertheless, it remains a clear misunderstanding.

1.11 An assertion that foreign nationals do not benefit from any protection for their privacy under US laws and practices is another mischaracterisation (albeit again, a widespread one). In fact, US law contains a number of protections for non-US persons whose communications may have been intercepted.

1.12 On 17 January 2014, the White House issued Presidential Policy Directive (PPD) no.28, which specifically extends privacy rights to non-US persons, stating:

---

[23] [***See Annex 24***]

[24] The Fourth Amendment to the US Constitution, incorporating the US constitutional right to privacy, states: *"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."*

[25] For example, the Advocate General in the recent CJEU case of *Schrems v Data Protection Commissioner C-362/14,* 6 October 2015 (***See Annex 25***) has asserted, it appears on the basis of findings made by the Irish High Court in proceedings to which the US Government was not party, that Prism "*allows the NSA unrestricted access to the mass data stored on servers located in the USA*": see [49] of the Advocate General's Opinion.

"All persons should be treated with dignity and respect, regardless of their nationality or wherever they may reside, and all persons have legitimate privacy interests in the handling of their personal information. US signals intelligence activities must, therefore, include appropriate safeguards for the personal information of all individuals, regardless of the nationality of the individual to whom the information pertains or where that individual resides."

1.13 Pursuant to PPD 28, the US intelligence agencies were directed to adopt data protection policies and procedures, applying to the retention, use, maintenance and dissemination of information about non-US persons, *"to the maximum extent feasible consistent with national security…to be applied equally to the personal information of all persons, regardless of nationality"* (emphasis added). The agencies were required to report on adoption of such policies within a year, and have done so.

1.14 Quite irrespective of the important provisions of PPD 28, a number of provisions of s.702 FISA, and other US surveillance laws, have protected the privacy of non-US persons since before PPD 28 came into effect. The position as regards these protections is summarised in PCLOB's 2 July Report at pp. 98-100, which states, as far as material:

"A number of provisions of section 702 [FISA], as well as provisions in other US surveillance laws, protect the privacy of U.S. and non-U.S. persons alike. Those protections can be found, for example, in (1) limitations on the scope of authorised surveillance under Section 702; (2) damages and other civil remedies that are available to subjects of unauthorised surveillance as well as sanctions that can be imposed on government employees who engage in such conduct; and (3) prohibitions on unauthorised secondary use and disclosure of information acquired pursuant to the Section 702 program. These sources of statutory privacy protections are discussed briefly.

The first important privacy protection provided to non-US persons is the statutory limitation on the scope of Section 702 surveillance, which requires that targeting be conducted only for purposes of collecting foreign intelligence information. The definition of foreign intelligence information purposes is limited to protecting against actual or potential attacks; protecting against international terrorism, and proliferation of weapons

of mass destruction; conducting counter-intelligence; and collecting information with respect to a foreign power or foreign territory that concerns US national defense or foreign affairs. Further limitations are imposed by the required certifications identifying the specific categories of foreign intelligence information, which are reviewed and approved by the FISC. These limitations do not permit unrestricted collection of information about foreigners.

The second group of statutory privacy protections for non-US persons are the penalties that apply to government employees who engage in improper information collection practices – penalties that apply whether the victim is a US person or a non-US person. Thus, if an intelligence analyst were to use the Section 702 program improperly to acquire information about a non-US person (for example, someone with whom he or she may have had a personal relationship), he or she could be subject not only to the loss of his or her employment, but to criminal prosecution. Finally, a non-US person who was a victim of a criminal violation of either FISA or the Wiretap Act could be entitled to civil damages and other remedies…

The third privacy protection covering non-US persons is the statutory restriction on improper secondary use found at 50 USC §1806, under which information acquired from FISA-related electronic surveillance may not "be used or disclosed by Federal officers or employees except for lawful purposes"…

Further, FISA provides special protections in connection with legal proceedings, under which an aggrieved person – a term that includes non-US persons – is required to be notified prior to the disclosure or use of any Section 702-related information in any federal or state court. The aggrieved person may then move to suppress the evidence on the grounds that it was unlawfully acquired and/or was not in conformity with the authorising Section 702 certification. Determinations regarding whether the Section 702 acquisition was lawful and authorised are made by a United States District Court, which has the authority to suppress any evidence that was unlawfully obtained or derived.

Finally, as a practical matter, non-US persons also benefit from the access and retention procedures required by the different agencies' minimisation and/or targeting procedures. While these procedures are legally required only for US persons, the cost and difficulty of identifying and removing US person information from a large body of data means that

typically the entire dataset is handled in compliance with the higher US person standards."

The UK intelligence services' receipt of intelligence material from foreign states

1.15 Mr Farr's witness statement made in the IPT proceedings (see ***Annex 3***) at §§15-25 sets out the high degree of unlikelihood that any government can obtain all the intelligence it needs from its own activities; and the immense importance and value to the UK's national interest of its ability to receive intelligence from the US[26]. As he then notes at §25, "*intelligence derived from communications and communications data obtained from foreign intelligence partners, and from the US intelligence agencies in particular, has led directly to the prevention of terrorist attacks and serious crime, and the saving of lives*".

1.16 The point is not confined to intelligence from the US. The UK has bilateral intelligence sharing relationships with a number of countries, including Council of Europe states, which are of very great importance to its national security interests. See the Anderson Report at §§10.31-10.32:

"As discussed at 7.66 above, the strongest partnership is the Five Eyes community involving the UK, USA, Canada, Australia and New Zealand. But there is bilateral sharing with many countries, not all of them in the established communities of the EU or the North Atlantic Treaty Organisation (NATO). Some of these relationships are broadly based where there is an enduring mutual interest. Others come together for a particular purpose such as a joint intervention.

These intelligence relationships are a vital contributor to [the Intelligence Services'] ability to provide the intelligence that the Government seeks…"

1.17 Mr Farr §§29-30 goes on to explain why no workable distinction can be made between the sharing of intercept intelligence, and other forms of intelligence, such as

[26] See too §§10.29-10.32 of the Anderson Report.

intelligence from covert human sources, so that the former should be separately regulated:

> *"From the point of view of the privacy interests of those individuals who are subject to investigative measures, I do not consider that a workable distinction can be drawn between such intelligence and [other forms of intelligence]…In particular, I do not consider that intelligence in the form of (or that is derived from) communications and communications data is in some general sense more personal or private than those other forms of intelligence. For instance, if an eavesdropping device is covertly installed in a target's home it may record conversations between family members that are more intimate and personal than those that might be recorded if the target's telephone were to be intercepted (and this example becomes even clearer if, for instance, the telephone in question is only used by the target to contact his criminal associates). To give a further example, a covert human intelligence source may be able to provide information about a target as a result of his or her friendship (or more intimate relationship) with the target that is more private than information that could be obtained from, for instance, intercepting the target's emails."*

1.18 GCHQ has obtained information from the US Government that the US Government obtained via Prism. The Government neither confirms nor denies that either the Security Service or the SIS has obtained from the US Government information obtained under Prism; or that any of the Intelligence Services have obtained from the US Government information obtained under Upstream. The reason for that NCND policy is that set out at Farr §§42-47.

Allegation of circumvention of domestic oversight regimes

1.19 Some of the intervenors have suggested (as if it were established fact) that receipt of intelligence material from the US via Prism and Upstream is used by the Intelligence Agencies as a means of circumventing domestic constraints on interception, imposed under RIPA[27]. That is entirely wrong. The Government has publicly confirmed that the receipt of such material is not and cannot lawfully be used as a means of circumventing domestic controls (see further below, under "Domestic Law and

[27] See e.g. the submissions of the International Commission of Jurists, pp. 3-4.

Practice"). Moreover, both the ISC and the Commissioner have stated on the basis of their own detailed investigations and sight of the evidence that this does not happen in practice. See the following (the effect of which is summarised at *Farr §§72-74, 124*):

(1) The ISC's Statement of 17 July 2013[28] on its investigation into the allegation that GCHQ used Prism as means of evading UK law (*"It has been alleged that GCHQ circumvented UK law by using the NSA's PRISM programme to access the content of private communications. From the evidence we have seen, we have concluded that this is unfounded"*).

(2) The Commissioner's 2013 Annual Report at §§6.8.1-6.8.6[29]. See in particular the question posed by the Commissioner and the unequivocal answer he gave at §6.8.1, together with his explanation at §6.8.6:

"8. Do British intelligence agencies receive from US agencies intercept material about British citizens which could not lawfully be acquired by intercept in the UK and vice versa and thereby circumvent domestic oversight regimes?

6.8.1 No. I have investigated the facts relevant to the allegations that have been published...

…

6.8.6 …information lawfully obtained by interception abroad is not necessarily available by interception to an interception agency here. In many cases it will not be available. If it is to be lawfully provided from abroad, it is sometimes appropriate for the interception agencies to apply explicitly by analogy the RIPA 2000 Part I principles of necessity and proportionality to its receipt here even though RIPA 2000 Part I does not strictly apply, because the interception did not take place in the UK by an UK agency. This is responsibly done in a number of appropriate circumstances by various of the agencies, and I am asked to review the consequent arrangements, although this may not be within my statutory remit."

1.20 To the extent that the Intervenors, or any sources that they cite, say otherwise, they speak without knowledge of the true position, and without the benefit of access to the evidence.

[28] See [***Annex 13***]
[29] See [***Annex 13***]

(2) The complaint about the alleged Tempora operation

The nature of interception under s.8(4) RIPA

1.21 The Government neither confirms nor denies the existence of the alleged Tempora interception operation, for the reasons set out at Farr §§42-47. However, the Government can state (and has previously stated) that it intercepts communications in "bulk" – that is, at the level of communications cables – pursuant to the lawful authority of warrants under s.8(4) RIPA. Such interception is described in general terms by the Commissioner in his Annual Reports of 2013 and 2014; in a report of the Intelligence and Security Committee of Parliament ("ISC") of 17 March 2015[30], *"Privacy and Security: A modern and transparent legal framework"* ("the ISC Report")[31] at §§49-77; and in a report of the Investigatory Powers Review of June 2015 by David Anderson QC, *"A Question of Trust"* ("the Anderson Report")[32] at chapter 10. The Commissioner, the ISC and Mr Anderson QC are independent of Government. All have been able to investigate the interception capabilities of the Intelligence Services in detail, with the full cooperation of the Services[33]. Each has engaged with, or taken evidence from, many interested parties outside government, including some of the

[30] See [***Annex 14***]
[31] See [***Annex 13***]
[32] See [***Annex 14***]
[33] See e.g. the Commissioner's 2014 Report at §1.6 (***See Annex 12***):
"I can report that I have full and unrestricted access to all of the information and material that I require, however sensitive, to undertake my review. I am in practice given such unrestricted access and all of my requests (of which there have been many) for information and access to material or systems are responded to in full. I have encountered no difficulty from any public authority or person in finding out anything that I consider to be needed to enable me to perform my statutory function."
See e.g. the ISC Report, "Key Findings", p.1, (v) (***See Annex 13***):
"Our Inquiry has involved a detailed investigation into the intrusive capabilities that are used by the UK intelligence and security Agencies. This Report contains an unprecedented amount of information about those capabilities…" and p.11, §12: *"In carrying out this Inquiry, we are satisfied that the Committee has been informed about the full range of Agency capabilities, how they are used and how they are authorized. We have sought to include as much of this information as possible in this Report with the intention that it will improve transparency and aid public understanding of the work of the Agencies".*
See too the Anderson Report, p.1, §4 (***See Annex 14***):
"In conducting my Review I have enjoyed unrestricted access at the highest level of security clearance, to the responsible Government Departments (chiefly the Home Office and FCO) and to the relevant public authorities including police, National Crime Agency and the three security and intelligence agencies: MI5, MI6 and GCHQ. I have balanced those contacts by engagement with service providers, independent technical experts, NGOs, academics, lawyers, judges and regulators, and by fact-finding visits to Berlin, California, Washington DC, Ottawa and Brussels."

Applicants in this case[34], for the purposes of drafting their Reports. The Government can confirm the factual accuracy of the Reports' accounts of the Intelligence Services' capabilities.

1.22 The effect of this, as Mr Anderson QC stated at §§14.39-40 of his Report, is that the UK's current regime for bulk interception has now been *"exhaustively considered over the past year or so"* not only in his Report, but also by the Commissioner, ISC and IPT (in the Liberty proceedings), so that *"some of the most senior judicial and political figures in the country have had the opportunity to analyse the regime and comment upon it"*.[35] It should be added, this analysis and comment - by contrast to much speculation in the press and elsewhere - has been made on the basis of access to and evidence from the Intelligence Services themselves, and balanced appraisal of the Intelligence Services' capacities, considering evidence and representations from (in the ISC's words) "*both sides of the debate*".

1.23 A number of important factual matters need to be noted about s.8(4) interception. **First**, GCHQ could theoretically access traffic from a small percentage of the 100,000 "bearers" (i.e. fibre optic cables) making up the core structure of the internet. However, the resources required to process the data involved means that at any one time GCHQ in fact only accesses a fraction of that small percentage of bearers it has the ability to access. Those bearers GCHQ accesses are chosen exclusively on the basis of the possible intelligence value of the traffic they carry and are authorised for access by warrant. See the summary of the position at §§57—58 of the ISC Report (the Report is redacted for reasons of national security, and the redactions below are as they appear in the Report):

[34] See e.g. the Commissioner's extensive summary of his engagement with the public and interested parties in Chapter 3 of his 2014 Annual Report, "*Transparency and Accountability*". See also Annex 4 to the Anderson Report, and §§13-15 of the ISC Report (***See Annex 13***).

[35] That position may be contrasted, for instance, with the EU Parliament's Resolution of 12 March 2014, upon which the Applicants heavily rely in their Update Submissions (see the Update Submissions, §§9-12). The UK Government (in common with a number of Member States) did not engage with the inquiry preceding the Resolution, so that to the extent it reached any conclusions about the UK's interception capabilities, they were not based upon any evidence at all from the Intelligence Services, or access to information held by the Services.

"57. The allegation arising from the NSA leaks is that GCHQ "hoover up" and collect all internet communications. Some of those who gave evidence to this Inquiry said "the Agencies are monitoring the whole stream all the time", referring to the "apparent ubiquity of surveillance".

58. We have explored whether this is the case. It is clear that both for legal reasons and due to resource constraints it is not: GCHQ cannot conduct indiscriminate blanket interception of all communications. It would be unlawful for them to do so, since it would not be necessary or proportionate, as required by RIPA. Moreover, GCHQ do not have the capacity to do so and can only cover a fraction of internet communications.

- *Of the 100,000 "bearers" which make up the core infrastructure of the internet, GCHQ could theoretically access communications traffic from a small percentage (***). These are chosen on the basis of the possible intelligence value of the traffic they carry.*
- *However, the resources required to process the vast quantity of data involved mean that, at any one time, GCHQ access only a fraction of the bearers that they have the ability to access – around ***. (Again, these are chosen exclusively on the basis of the possible intelligence value of the traffic they carry).*
- *In practice, GCHQ therefore access only a very small percentage (around ***) of the internet bearers at any one time.*
- *Even then, this does not mean that GCHQ are collecting and storing all of the communications carried on these bearers…"*

1.24 Thus, the suggestion that GHCQ intercepts all communications entering and exiting the United Kingdom is simply wrong[36].

1.25 Specifically, when conducting interception under a s.8(4) warrant, knowledge of the way in which communications are routed over the internet is combined with regular surveys of internet traffic to identify those bearers that are most likely to contain external communications that will meet the descriptions of material certified for interception by the Secretary of State under s.8(4) RIPA: Farr §154. See too §6.7 of the Code (which requires this approach to be taken as a matter of law).

[36] See e.g. the Application Form Statement of Facts at §2(1), p4.

1.26 **Secondly**, GCHQ does not conduct "untargeted" surveillance of communications or communications data, intercepted pursuant to a s.8(4) warrant. (i.e. any selection of communications for examination is undertaken on the basis that they match selection rules used to find those communications of maximum intelligence interest). So, again, any suggestion that GCHQ engages in 'blanket' surveillance is wholly incorrect.

(1) One major processing system operated by GCHQ on all the bearers it has chosen to access under s.8(4) RIPA compares the traffic carried by the bearers against a list of specific "simple selectors" – that is, specific identifiers relating to an individual target, such as (for example) an email address. Any communications which match the selectors are automatically collected. All other communications are automatically discarded. See the ISC Report, §§61-63. As the ISC Report states at §64: *"In practice, while this process has been described as bulk interception because of the numbers of communications it covers, it is nevertheless targeted since the selectors used relate to individual targets"*.

(2) Another major processing system enables GCHQ to search for communications using more complicated criteria (for example, selectors with three or four different elements). This process operates against a far smaller number of bearers, which are chosen from the total number of bearers intercepted by GCHQ as those most likely to carry communications of intelligence interest: see the ISC Report, §§65-66.

(3) Under this second system, a set of "selection rules" is applied to communications travelling over a bearer. The system automatically discards the majority of traffic on the targeted bearers, which does not meet those rules (the filtering stage). There is then a further stage, before analysts can examine or read any communications (selection for examination). This involves GCHQ conducting automated complex searches, to draw out communications most likely to be of greatest intelligence value, which relate to GCHQ's statutory functions, and the selection of which meets conditions of necessity and proportionality. Those searches generate an index. Only

items contained in the index can potentially be examined by analysts. All other items cannot be searched for, examined or read. See the ISC Report, §§67-73.

(4) Thus, what is filtered out by the application of automated searches is immediately discarded and ceases to be available. As stated by the Commissioner at §6.5.55 of his 2013 Report[37]:

"What remains after filtering (if anything) will be material which is strongly likely to include individual communications which may properly and lawfully be examined under the section 8(4) process. Examination is then effected by search criteria constructed to comply with the section 8(4) process."

1.27 **Thirdly**, only a fraction of those communications selected for possible examination by either of the processing systems set out above is ever looked at by an analyst.

(1) In relation to communications obtained via the use of "simple selectors", a "triage" process is applied, to determine which will be of most use. This triage process means that the vast majority of the items collected in this way are never looked at by an analyst, even where they are known to relate to specific targets.

(2) In relation to communications obtained via the application of complex search terms, items are presented to analysts as a series of indexes in tabular form showing the result of searches. To access the full content of any item, the analyst has to decide to open the specific item of interest based on the information in the index, using their judgment and experience. In simple terms, this can be considered as an exercise similar to that conducted when deciding what search results to examine, from a list compiled by a search engine such as Bing or Google. The remainder of the potentially relevant items are never opened or read by analysts.

(3) In summary, as stated by the ISC, the communications selected for examination *"are only the ones considered to be of the highest intelligence value.*

[37] See [***Annex 11***]

Only the communications of suspected criminals or national security targets are deliberately selected for examination": see the ISC Report, §77.

1.28 That final observation is derived from the conclusion of the Commissioner in his Annual Report for 2013 at §6.7.5:

> *"I am…personally quite clear that any member of the public who does not associate with potential terrorists or serious criminals or individuals who are involved in actions which could raise national security issues for the UK can be assured that none of the interception agencies which I inspect has the slightest interest in examining their emails, their phone or postal communications or their use of the internet, and they do not do so to any extent which could reasonably be regarded as significant."*

The rationale for and utility of s.8(4) interception

1.29 There are two fundamental reasons why it is necessary to intercept the contents of bearers for wanted external communications, both of which ultimately derive from the substantial practical difference between the Government's control over and powers to investigate individuals and organisations within the UK, and those that operate outside that jurisdiction[38] (see e.g. the Anderson Report at §10.22[39]):

(1) Bulk interception is critical both for the discovery of threats, and for the discovery of targets who may be responsible for threats. When acquiring intelligence on activities overseas, the Intelligence Services do not have the same ability to identify targets or threats that they possess within the UK. For example, small items of intelligence (such as a suspect location) may be used to find links leading to a target overseas, or to discovery of a threat; but that can only be done, if the Services have access to a substantial volume of communications through which to search for those links.

[38] See Mr Farr at §§143-147 for a summary of those differences.
[39] [***Annex 14***]

(2) Even where the Intelligence Services know the identity of targets, their ability to understand what communications bearers those targets will use is limited, and their ability to access those bearers is not guaranteed. Subjects of interest are very likely to use a variety of different means of communication, and to change those means frequently. Moreover, electronic communications do not traverse the internet by routes that can necessarily be predicted. Communications will not take the geographically shortest route between sender and recipient, but the route that is most efficient, as determined by factors such as the cost of transmission, and the volume of traffic passing over particular parts of the internet at particular times of day. So in order to obtain even a small proportion of the communications of known targets overseas, it is necessary for the Services to intercept a selection of bearers, and to scan the contents of all those bearers for the wanted communications.

1.30 In addition, there are technical reasons why it is necessary to intercept the contents of a bearer, in order to extract specific communications. The precise position is complex, and the technical details are sensitive, but the basic position is that communications sent over the internet are broken down into small pieces, known as "packets", which are then transmitted separately, often through different routes, to the recipient, where the message is reassembled. It follows that in order to intercept a given communication that is travelling over the internet (say, an email), any intercepting agency will need to obtain all the packets associated with that communication, and reassemble them.

1.31 Thus, if an intercepting agency needs (for example) to obtain communications sent to an individual (C) in Syria, whilst they are being transmitted over the internet, and has access to a given bearer down which such communications may travel, the intercepting agency will need to intercept all communications that are being transmitted over that bearer – at least for a short time – in order to discover whether any are intended for C. Further, since the packets associated with a given communication may take different routes to reach their common destination, it may be necessary to intercept all communications over more than one bearer to maximise the chance of identifying and obtaining the communications being sent to C.

1.32 In summary, as Mr Farr stated at §149[40]:

> *"Taking these considerations in the round, it will be apparent that the only practical way in which the Government can ensure that it is able to obtain at least a fraction of the type of communication in which it is interested is to provide for the interception of a large volume of communications, and the subsequent selection of a small fraction of those communications for examination by the application of relevant selectors."*

1.33 The Commissioner, the ISC Report, and the Anderson Report have all recently examined in detail the need for bulk interception of communications under s.8(4) RIPA (or equivalent powers) in the interests of the UK's national security. All have concluded there is no doubt that such a capability is valuable, because it meets intelligence needs, which cannot be satisfied by any other reasonable means.

(1) The Commissioner's Annual Report of 2013 asked at §6.4.49 whether there were other reasonable but less intrusive means of obtaining needed external communications, and concluded at §6.5.51[41]:

> *"I am satisfied that at present there are no other reasonable means that would enable the interception agencies to have access to external communications which the Secretary of State judges it is necessary for them to obtain for a statutory purpose under the section 8(4) procedure. This is a sensitive matter of considerable technical complexity which I have investigated in detail."*

Further, the Commissioner, having pointed out that there was a policy question whether the Intelligence Services should continue to be enabled to intercept external communications under s.8(4) RIPA, stated that he thought it "*obvious*" that, subject to sufficient safeguards, they should be: §6.5.56.

(2) The ISC Report stated as follows (see [***Annex 13***]):

[40] [***See Annex 3***]
[41] [***See Annex 11***]

"It is essential that the Agencies can "discover" unknown threats. This is not just about identifying individuals who are responsible for threats, it is about finding those threats in the first place. Targeted techniques only work on "known" threats: bulk techniques (which themselves involve a degree of filtering and targeting) are essential if the Agencies are to discover those threats." (§77(K))

"GCHQ have provided case studies to the Committee demonstrating the effectiveness of their bulk interception capabilities. Unfortunately, these examples cannot be published, even in redacted form, without significant risk to GCHQ's capabilities, and consequential damage to the national security of the UK. We can, however, confirm that they refer to complex problems relating directly to some of the UK's highest priority intelligence requirements." (§81)

"The examples GCHQ have provided, together with the other evidence we have taken, have satisfied the Committee that GCHQ's bulk interception capability is used primarily to find patterns in, or characteristics of, online communications which indicate involvement in threats to national security. The people involved in these communications may be already known, in which case valuable extra intelligence may be obtained (e.g. a new person in a terrorist network, a new location to be monitored, or a new selector to be targeted). In other cases, it exposes previously unknown individuals or plots that threaten our security which would not otherwise be detected.

L. We are satisfied that current legislative arrangements and practice are designed to prevent innocent people's communications being read. Based on that understanding, we acknowledge that GCHQ's bulk interception is a valuable capability that should remain available to them." (§§90, 90(L))

(3) The Anderson Report commented on the uses of bulk interception at §§7.22-7.27[42], noting the importance of bulk interception for target discovery; and observing that this did not mean suspicion played no part in the selection of communications channels for interception, or in the design of searches conducted on intercepted material. In particular:

[42] ***[See Annex 14]***

At §7.25, Mr Anderson QC stated:

> *"GCHQ explained that its bulk access capabilities are the critical enabler for the cyber defence of the UK, providing the vast majority of all reporting on cyber threats and the basis for counter-activity. In a recent two week period bulk access provided visibility to GCHQ of 96 distinct cyber-attack campaigns. Bulk access is also the only means by which GCHQ can obtain the information it needs to develop effective responses to these attacks."*

At §7.26, Mr Anderson QC stated in summary that it was for the courts to decide whether such bulk interception was proportionate, but that he was in no doubt about the value of its role:

> *"GCHQ provided case studies to the ISC to demonstrate the effectiveness of its bulk interception capabilities. I have been provided with the same case studies and with other detailed examples, on which I have had the opportunity to interrogate GCHQ analysts at length and by reference to detailed intelligence reports based on the analysis of bulk data. They leave me in not the slightest doubt that bulk interception, as it is currently practised, has a valuable role to play in protecting national security."*

(4) At §14.45, Mr Anderson QC concluded[43]:

> *"Whether or not the s.8(4) regime is proportionate for the purposes of ECHR Article 8 is an issue awaiting determination by the ECHR. It is not my function to offer a legal assessment, particularly in a case that is under*

[43] At §14.44, Mr Anderson also had observations to make about a draft resolution from the Council of Europe's Committee on Legal Affairs and Human Rights, upon which the Applicants heavily rely in their Update Submissions (see e.g. §16 of the Submissions). Mr Anderson QC adverted to *"contrasting reports"* from the Council of Europe on bulk data collection. He compared the findings and resolution of the Committee on Legal Affairs and Human Rights, which cast doubt on the efficacy of bulk interception, with a report of April 2015 from the European Commission for Democracy through Law. He observed that the notion that bulk interception is ineffective "*is contradicted by the detailed examples I have been shown at GCHQ*"'. He pointed out that aspects of the methodology upon which the Committee's findings were made "*seem debatable*", and failed to take into account "*the potential of safeguards, regulation and oversight*". He commented that the April 2015 report was drafted "*in considerably more moderate (and on the basis of what I have seen realistic) terms*". (See Annex 14)

> *consideration by a senior court. But on the basis of what I have learned, there is no cause for me either to disagree with the factual conclusions expressed in recent months by [the Commissioner], the IPT or the ISC, or to recommend that bulk collection in its current form should cease. Indeed its utility, particularly in fighting terrorism in the years since the London bombings of 2005, has been made clear to me through the presentation of case studies and contemporaneous documents on which I have had the opportunity to interrogate analysts and other GCHQ staff."*

1.34 The Anderson Report contains (at Annex 9[44]) six "case study" examples of intelligence from the bulk interception of communications. The importance of those examples speaks for itself. In summary, they are:

(1) The triggering of a manhunt for a known terrorist linked to previous attacks on UK citizens, at a time when other intelligence sources had gone cold, and the highlighting of links between the terrorist and extremists in the UK, ultimately enabling the successful disruption of a terrorist network ("Case Study 1");

(2) The identification in 2010 of an airline worker with links to Al Qaida, who had offered to use his airport access to launch a terrorist attack from the UK, in circumstances where his identification would have been highly unlikely without access to bulk data ("Case Study 2");

(3) The identification in 2010 of an Al Qaida plot to send out operatives to act as sleeper cells in Europe, and prepare waves of attacks. The operatives were identified by querying bulk data for specific patterns ("Case Study 3");

(4) The discovery in 2011 of a network of extremists in the UK who had travelled to Pakistan for extremist training, and the discovery that they had made contact with Al Qaida ("Case Study 4");

(5) Analysis of bulk data to track two men overseas who had used the world wide web to blackmail hundreds of children across the world. GCHQ was able to confirm their names and locations, leading to their arrest and jailing in their home country ("Case Study 5");

[44] [***See Annex 14***]

(6) The discovery in 2014 of links between known ISIL extremists in Syria and a previously unidentified individual, preventing a bomb plot in mainland Europe which was materially ready to proceed. Bulk data was the trigger for the investigation ("Case Study 6").

1.35 Quite aside from the direct threats to life set out above, bulk interception is also the only way in which the Intelligence Services can realistically discover cyber threats: a danger which potentially affects almost every person in the UK using a computer. The scale of the issue is one to which Mr Anderson QC adverted, when he pointed out that over a 2-week period bulk access had enabled GCHQ to discover 96 separate cyber-attack campaigns. The internet is an intrinsically insecure environment, with billions of computers constantly running millions of complex programmes. PwC's 2015 Information security breaches survey (See Annex 56) reported that 90% of large organisations and 74% of small businesses had a security breach in the period covered by the report; the average cost of the worst serious breach ranged from £1.46m to £3.14m for large organisations, and £75,000 to £311,000 for small businesses.

Internal and external communications

1.36 Interception under a s. 8(4) warrant is directed at "external communications" of a description to which the warrant relates: that is, at communications sent or received outside the British Islands (see s.20 RIPA, and see further below, under "domestic law and practice"). But the fact that electronic communications may take any route to reach their destination inevitably means that a proportion of communications flowing over a bearer between the UK and another State will consist of "internal communications": i.e., communications between persons located in the British Islands.

1.37 It was well understood by Parliament at the time RIPA was enacted that interception of a bearer for wanted external communications would necessarily entail the interception of at least some internal communications. See Lord Bassam of Brighton

(the relevant Government Minister) in the House of Lords in July 2000[45] (cited at Farr §130):

> *"It is just not possible to ensure that only external communications are intercepted. That is because modern communications are often routed in ways that are not all intuitively obvious…An internal communication – say, a message from London to Birmingham – may be handled on its journey by Internet service providers in, perhaps, two different countries outside the United Kingdom. We understand that. The communication might therefore be found on a link between those two foreign countries. Such a link should clearly be treated as external, yet it would contain at least this one internal communication. There is no way of filtering that out without intercepting the whole link, including the internal communication."*

1.38 Nevertheless, when conducting interception under a s.8(4) warrant, knowledge of the way in which communications are routed over the internet is combined with regular surveys of internet traffic to identify those bearers that are most likely to contain external communications that will meet the descriptions of material certified by the Secretary of State as necessary to intercept. While this approach may lead to the interception of some communications that are not external, s.8(4) operations are conducted in a way that keeps this to the minimum necessary to achieve the objective of intercepting wanted external communications: see Farr §154.

1.39 The Commissioner's findings are entirely consistent with the above position: see his 2013 Annual Report at §§6.5.52-6.5.54:

> *"6.5.52 …I am satisfied from extensive practical and technical information provided to me that it is not at the moment technically feasible to intercept external communications without a risk that some internal communications may also be initially intercepted. This was contemplated and legitimised by s.5(6)(a) of RIPA 2000 which embraces*

[45] Lord Bassam of Brighton introduced the Regulation of Investigatory Powers Bill (i.e. the Bill that became RIPA) on behalf of the Government in the House of Lords. The quotation is from the Lords Committee, Hansard, 12 July 2000 at column 323. See [***Annex 26***]

> *"all such conduct (including the interception of communications not identified by the warrant) as it is necessary to undertake in order to do what is expressly authorised or required by the warrant."*
>
> *6.6.53 Thus the unintended but unavoidable initial interception of some internal communications under a section 8(4) warrant is lawful. Reference to Hansard House of Lords Debates for 12 July 2000 shows that this was well appreciated in Parliament when the bill which became RIPA 2000 was going through Parliament.*
>
> *6.5.54 However, the extent to which this material, lawfully intercepted, may be lawfully examined is strictly limited by the safeguards in [section 16 RIPA]…And in any event my investigations indicate that the volume of internal communications lawfully intercepted is likely to be an extremely small percentage of the totality of internal communications and of the total available to an interception agency under a section 8(4) warrant."*

1.40 Mr Farr gave various examples of communications which he regarded as "internal", and those which he regarded as "external" at Farr §§134-138. For example, he indicated that a "Google" search was in effect a communication between the person conducting the search, and Google's index of web pages, hosted on its servers; and that because those servers were in general based in the US, such a search might well be an external communication. The Applicants have asserted that there is no practical distinction between internal and external communications and that the distinction has been "fundamentally eroded" and is "unclear"[46]. Those criticisms are misplaced; but more importantly, the Applicants have neglected to mention Mr Farr's observation that the question whether a particular communication is internal or external is entirely distinct from (and irrelevant to) the question whether it can lawfully be selected for examination: see Farr §§139-141, 157-158. (That point is expanded upon further below, in answer to the Applicants' criticism of the definition of "external communications": see §§ 4.66-4.76.

(3) Proceedings in the IPT

[46] see §45 of the Applicants' Additional Submissions on the Facts and Complaints.

1.41 The Applicants brought claims in the IPT in 2013 ("the Liberty proceedings"), specifically challenging the lawfulness of the UK's intelligence sharing and s.8(4) regimes, in the context of allegations about Prism, Upstream, and the alleged Tempora operation. While there are some minor differences between the allegations made in this Application and those made in the Liberty Proceedings, the IPT had the opportunity in the Liberty Proceedings to consider and rule upon the principal issues that the Applicants now raise.

1.42 The IPT, which consisted in this case of five experienced members, including two High Court judges, held a 5-day open hearing in July 2014 at which issues of law were considered on assumed facts. It also:

(1) considered additional legal issues in a series of further open hearings;
(2) considered the internal policies and practices of the relevant Intelligence Services in further open and (to the extent that such policies and practices could not be publicly disclosed for reasons of national security) closed hearings; and
(3) considered evidence which could not be disclosed for reasons of national security in closed hearings. Such evidence concerned he operation of the intelligence sharing and s.8(4) regimes; and matters of proportionality (both of the regime and of the interception of the claimants' communications (if any)).

1.43 Throughout the hearings, the claimants were represented by teams of experienced Counsel, and the IPT had the benefit of assistance from Counsel to the Tribunal. Following those hearings, the IPT issued a series of open judgments, as set out below.

Judgment of 5 December 2014

1.44 In its judgment of 5 December 2014 ("The 5 December Judgment"[47]) the IPT considered a series of questions concerning the lawfulness of the Intelligence Sharing Regime and the s.8(4) Regime. The questions were answered on the agreed, but

[47] [See Annex 15]

assumed, factual premises that the claimants' communications (i) might in principle have been obtained via Prism or Upstream, and provided to the Intelligence Services; and (ii) might in principle have been intercepted and examined under the s.8(4) Regime[48]. The IPT adopted the shorthand "Prism issue" and "s.8(4) issue" for the matters arising under each head.

1.45 The IPT found as follows in relation to the **Prism** issue:

(1) The Prism issue engaged Article 8 ECHR, and required that any interference with the claimants' communications be "in accordance with the law" on the basis of the principles in *Malone v UK* and *Bykov v Russia* (app. 4378/02, GC, 10 March 2009): see judgment, §§37-38.

(2) For the purposes of the "in accordance with the law" test, appropriate rules or arrangements governing intelligence sharing should exist and be publicly known and confirmed to exist, with their content sufficiently signposted; and they should be subject to proper oversight. However, they did not need to be in a code or statute: see judgment, §41.

(3) The IPT was entitled to look at the Intelligence Services' internal policies and procedures that were not made public – i.e. "below the waterline" - in order to determine whether the Intelligence Sharing regime offered adequate safeguards against abuse: see judgment, §50.

(4) Certain details of those internal policies and procedures could properly be made open without damaging national security. The respondents agreed to make voluntary disclosure of those details, which were recorded in the judgment ("the Disclosure"): see judgment, §§47-48. (The Disclosure is now reflected in the Code, the current version of which postdates the IPT's judgment. See in particular §§7.8-7.9 and chapter 12 of the Code.)

(5) The effect of the internal policies and procedures was that the same requirements and internal safeguards were applied to all data, solicited or unsolicited, received pursuant to Prism or Upstream, as applied to material obtained under RIPA by the Intelligence Services themselves: see judgment, §54.

[48] i.e. pursuant to bulk interception under a s.8(4) warrant

(6) In sum, in light of the Disclosure, the respondents' arrangements for the purposes of the Prism issue were in accordance with the law under Articles 8 and 10 ECHR. There were adequate arrangements "below the waterline", which were sufficiently signposted by virtue of (i) the applicable statutory framework; (ii) statements of the ISC and Commissioner concerning the Prism issue (as to which, see §1.19(2), §3.24 and §3.26 above), and (iii) the Disclosure itself: judgment, §55.

(7) The only remaining issue was whether there was a breach of Article 8 ECHR prior to the judgment, because the Disclosure had not been made. That issue would be considered further, in light of submissions from the parties: see judgment, §154.

1.46 In relation to the **s.8(4)** issue:

(1) The IPT first considered whether the difficulty of determining the difference between external and internal communications, whether as a theoretical or practical matter, was such as to render the s.8(4) regime not in accordance with the law. The answer was no: see judgment, §§93102.

(2) The requirement under s.16 RIPA that the Secretary of State certify the necessity of examining communications intercepted under a s.8(4) warrant, if they are to be examined using a factor referable to an individual known to be in the UK, was an important and adequate safeguard. It was also justified and proportionate not to extend that safeguard to communications data. The *Weber* criteria extend to communications data, but those criteria were met without reference to the safeguards in s.16 RIPA, and it was justified and proportionate to extend greater protection to the content of communications than to communications data: see judgment, §§103-114.

(3) The s.8(4) system, leaving aside the effect of s.16 RIPA, sufficiently complied with the *Weber* criteria[49], and was in accordance with the law. Moreover, the ECtHR's own conclusions on the oversight mechanisms under RIPA in *Kennedy* endorsed that conclusion: see judgment, §§117-140.

[49] I.e. the six criteria set out at §95 of *Weber and Saravia v Germany*

(4) Any indirect discrimination within the s.8(4) system by virtue of a distinction in the protections afforded to persons within the UK and outside the UK was proportionate and justified: see judgment, §§141-148.

(5) No distinction fell to be made between the analysis for the purposes of Article 8 ECHR and Article 10 ECHR: see judgment, §§149-152.

1.47 The IPT stated in conclusion at §§158-159 of the judgment:

> *"158. Technology in the surveillance field appears to be advancing at break-neck speed. This has given rise to submissions that the UK legislation has failed to keep abreast of the consequences of these advances, and is ill fitted to do so; and that in any event Parliament has failed to provide safeguards adequate to meet those developments. All this inevitably creates considerable tension between the competing interests, and the "Snowden revelations" in particular have led to the impression voiced in some quarters that the law in some way permits the Intelligence Services carte blanche to do what they will. We are satisfied that this is not the case.*
>
> *159. We can be satisfied that, as addressed and disclosed in this judgment, in this sensitive field of national security, in relation to the areas addressed in this case, the law gives individuals an adequate indication as to the circumstances in which and the conditions upon which the Intelligence Services are entitled to resort to interception, or make use of intercept."*

Judgment of 6 February 2015

1.48 In a judgment of 6 February 2015 ("the 6 February Judgment")[50], the IPT considered the outstanding issue in §154 of its 5 December Judgment, namely whether prior to the Disclosure the Intelligence Sharing regime was in accordance with the law. It held that it was not, because without the Disclosure the internal arrangements for handling of material received via Prism/Upstream (if any) were inadequately signposted. However, it declared that in light of the Disclosure the regime was now in accordance with the law.

[50] [***See Annex 27***]

Judgment of 22 June 2015

1.49 The IPT's judgment of 22 June 2015 ("the 22 June Judgment")[51] concerned the issue whether there had in fact been unlawful conduct in relation to any of the claimants' communications under either of the Intelligence Sharing or the s.8(4) regimes. In determining that issue, the IPT considered proportionality both as it arose specifically in relation to the claimants' communications, and as it arose in relation to the s.8(4) Regime as a whole (i.e. what the IPT described as "systemic proportionality"): see judgment, §3. The issue of "systemic proportionality" arose at this point because, if it was generally disproportionate e.g. to intercept the entirety of the contents of a fibre optic cable, all the claimants could in principle have been entitled to a remedy, on the basis that their communications of no intelligence interest would or might have been so intercepted, even if immediately discarded.

1.50 The IPT concluded that there had been unlawful conduct in relation to two of the claimants, whose communications had been intercepted and selected for examination under the s.8(4) Regime: namely, the Legal Resources Centre and Amnesty International[52]. In each case, the unlawful conduct in question was "technical", in that it had caused the claimants no prejudice (so that a declaration constituted just satisfaction):

(1) Email communications associated with Amnesty International[53] had been lawfully and proportionately intercepted and selected for examination by GCHQ. They had in error been retained for longer than permitted under GCHQ's internal policies. So their retention was not "in accordance with the law" for the purposes of Article 8 ECHR. However, they were not accessed after the expiry of the relevant time limit: see judgment, §14.

[51] [***See Annex 28***]
[52] The IPT's 22 June Judgment erroneously stated that the finding in favour of Amnesty International was a finding in favour of the Egyptian Initiative for Personal Rights. That mistaken attribution was corrected by the IPT in a letter of 2 July 2015 (See Annex 29).
[53] The references to the Egyptian Initiative for Personal Rights in the 22 June Judgment should be references to Amnesty International. See the IPT's letter of 2 July 2015. The 22 June Judgment did not reveal whether or not the particular email address or addresses associated with the claimants had themselves been the target of the interception, or whether they had simply been in communication with the target of the interception.

(2) Communications from an email address associated with the Legal Resource Centre had been lawfully and proportionately intercepted, and proportionately selected for examination. However, GCHQ's internal procedure for selection of the communications for examination had in error not been followed. Accordingly, the selection of the communications for examination was not "in accordance with the law" for the purposes of Article 8 ECHR. Notwithstanding that, no use whatsoever had been made of any intercepted material, nor any record retained: see judgment, §15.

1.51 The IPT stated at §18:

> *"The Tribunal is concerned that steps should be taken to ensure that neither of the breaches of procedure referred to in this Determination occurs again. For the avoidance of doubt, the Tribunal makes it clear that it will be making a closed report to the Prime Minister pursuant to s.68(5) of RIPA."*

2 PART 2 - DOMESTIC LAW AND PRACTICE

The Intelligence Sharing Regime

2.1 The Intelligence Sharing Regime is contained principally in the following statutes, as supplemented by the Code (which itself reflects the IPT's 5 December and 6 February Judgments):

(1) the SSA and the ISA, as read with the CTA;
(2) the HRA;
(3) the DPA; and
(4) the OSA.

In addition, the provisions of RIPA are relevant as regards the scope of the power of UK public authorities to obtain communications and/or communications data from foreign intelligence agencies.

The SSA, the ISA and the CTA

2.2 Section 1 SSA provides in relevant part:

> *"(2) The function of the [Security] Service shall be the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means.*
> *(3) It shall also be the function of the [Security] Service to safeguard the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands.*
> *(4) It shall also be the function of the [Security] Service to act in support of the activities of police forces, the National Crime Agency and other law enforcement agencies in the prevention and detection[54] of serious crime."*

2.3 The operations of the Security Service are under the control of the Director-General, who is appointed by the Secretary of State (s. 2(1) SSA). By s. 2(2)(a), it is the duty of the Director-General to ensure:

> *"...that there are arrangements for securing that no information is obtained by the Service except so far as necessary for the proper discharge of its functions or disclosed by it except so far as necessary for that purpose or for the purpose of the prevention or detection of serious crime or for the purpose of any criminal proceedings..."*

See also s. 19(3) CTA.[55]

2.4 Subject to s. 1(2) of the ISA, the functions of SIS are, by s. 1(1) of the ISA:

> *"(a) to obtain and provide information relating to the actions or intentions of*

[54] By s. 1(5) of the SSA, the definitions of "prevention" and "detection" in s. 81(5) of RIPA apply for the purposes of the SSA.
[55] By s. 19(3), information obtained by the Security Service for the purposes of any of its functions "*may be disclosed by it - (a) for the purpose of the proper discharge of its functions, (b) for the purpose of the prevention or detection of serious crime, or (c) for the purpose of any criminal proceedings*."

persons outside the British Islands; and

(b) to perform other tasks relating to the actions or intentions of such persons."

2.5 By s. 1(2) of the ISA:

> *"The functions of the Intelligence Service shall be exercisable only –*
>
> *(a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or*
>
> *(b) in the interests of the economic well-being of the United Kingdom; or*
>
> *(c) in support of the prevention or detection of serious crime."*

2.6 The operations of SIS are under the control of the Chief of the Intelligence Service, who is appointed by the Secretary of State (s. 2(1) ISA). By s. 2(2)(a), it is the duty of the Chief of the Intelligence Service to ensure:

> *"... that there are arrangements for securing that no information is obtained by the Intelligence Service except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary –*
>
> *(i) for that purpose;*
>
> *(ii) in the interests of national security;*
>
> *(iii) for the purpose of the prevention or detection of serious crime; or*
>
> *(iv) for the purpose of any criminal proceedings ..."*

See also s. 19(4) CTA.[56]

2.7 By s. 3(1)(a) of the ISA, the functions of GCHQ include the following:

> *"... to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material*

[56] By s. 19(4), information obtained by SIS for the purposes of any of its functions "*may be disclosed by it - (a) for the purpose of the proper discharge of its functions, (b) in the interests of national security, (c) for the purpose of the prevention or detection of serious crime, or (d) for the purpose of any criminal proceedings*."

…."

2.8 By s. 3(2) of the ISA, these functions are only exercisable:

> "*(a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or*
>
> *(b) in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands; or*
>
> *(c) in support of the prevention or detection of serious crime*."

2.9 GCHQ's operations are under the control of a Director, who is appointed by the Secretary of State (s. 4(1)). By s. 4(2)(a), it is the duty of the Director to ensure:

> *"... that there are arrangements for securing that no information is obtained by GCHQ except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary for that purpose or for the purpose of any criminal proceedings ..."*

See also s. 19(5) of the CTA.[57]

2.10 Thus, specific statutory limits are imposed on the information that each of the Intelligence Services can obtain, and on the information that each can disclose. Further, these statutory limits do not simply apply to the obtaining of information from other persons in the United Kingdom or to the disclosing of information to such persons: they apply equally to obtaining information from / disclosing information to persons abroad, including foreign intelligence agencies. In addition, the term "information" is a very broad one, and is capable of covering *e.g.* communications and communications data that a foreign intelligence agency has obtained.

2.11 By s. 19(2) CTA:

> "*Information obtained by any of the intelligence services in connection with the exercise of any of its functions may be used by that service in connection with the*

[57] By s. 19(5), information obtained by GCHQ for the purposes of any of its functions "*may be disclosed by it - (a) for the purpose of the proper discharge of its functions, or (b) for the purpose of any criminal proceedings.*"

exercise of any of its other functions."

It is thus clear that *e.g.* information that is obtained by the Security Service for national security purposes (by reference to s. 1(2) SSA) can subsequently be used (including disclosed) by the Security Service to support the activities of the police in the prevention and detection of serious crime (pursuant to s. 1(4) SSA).

The HRA

2.12 Art. 8 ECHR is a "Convention right" for the purposes of the HRA: s. 1(1) HRA. Art. 10 of the ECHR is similarly a Convention right (and is similarly set out in Sch. 1 to the HRA).

2.13 By s. 6(1) HRA: "*It is unlawful for a public authority to act in a way which is incompatible with a Convention right*." Each of the Intelligence Services is a public authority for this purpose. Thus, when undertaking <u>any</u> activity that interferes with Art. 8 rights (such as obtaining communications or communications data, or retaining, using or disclosing such information), the Intelligence Services must (among other things) act proportionately, having regard to the legitimate aim pursued,[58] pursuant to s. 6(1) HRA. Further, the same obligation to act proportionately is imposed insofar as the contemplated activity interferences with Art. 10 rights.

2.14 Section 7(1) HRA provides in relevant part:

> "*A person who claims that a public authority has acted (or proposes to act) in a way which is made unlawful by section 6(1) may –*
>
> *(a) bring proceedings against the authority under this Act in the appropriate court or tribunal ....*"

The DPA

2.15 Each of the Intelligence Services is a "data controller" (as defined in s. 1(1) DPA) in relation to all the personal data (as defined in s. 1(1) DPA) that it holds.

[58] The permissible aims being specified in the SSA and the ISA, respectively.

2.16 As a data controller, each of the Intelligence Services is in general required by s. 4(4) DPA to comply with the data protection principles in Part I of Sch. 1 to the DPA. That obligation is subject to ss. 27(1) and 28(1) DPA, which exempt personal data from (among other things) the data protection principles if the exemption "*is required for the purpose of safeguarding national security*". By s. 28(2) DPA, a Minister may certify that exemption from the data protection principles is so required. Copies of the ministerial certificates for each of the Intelligence Services are available on request. Those certificates (see ***Annex 30***) certify that personal data that are processed in performance of the Intelligence Services' functions are exempt from the first, second and eighth data protection principles (and are also exempt in part from the sixth data protection principle). Thus the certificates do <u>not</u> exempt the Intelligence Services from their obligation to comply, *inter alia*, with the fifth and seventh data protection principles, which provide:

> "*5.Personal data processed*[59] *for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. …*
>
> *7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*"[60]

2.17 Insofar as the obtaining of an item of information by any of the Intelligence Services from a foreign intelligence agency amounts to an interference with Art. 8 rights, that item of information will in general amount to personal data. Accordingly, when the Intelligence Services obtain any such information from a foreign intelligence agency, they are obliged by the DPA:

(1) not to keep that data for longer than is necessary having regard to the purposes for which they have been obtained and are being retained/used; and

[59] The term "processing" is broadly defined in s. 1(1) of the DPA to include (among other things), obtaining, recording and using.
[60] The content of the obligation imposed by the seventh data protection principle is further elaborated in §§9-12 of Part II of Sch. 1 to the DPA.

(2) to take appropriate technical and organisational measures to guard against unauthorised or unlawful processing of the data in question and against accidental loss of the data in question. (See also, in this regard, §2.19 below).

The OSA

2.18 A member of the Intelligence Services commits an offence if "*without lawful authority he discloses any information, document or other article relating to security or intelligence which is or has been in his possession by virtue of his position as a member of any of those services*": s. 1(1) OSA. A disclosure is made with lawful authority if, and only if, it is made in accordance with the member's official duty (s. 7(1) OSA). Thus, a disclosure of information by a member of the Intelligence Services that is *e.g.* in breach of the relevant "arrangements" (under, as the case may be, s. 2(2)(a) SSA, s. 2(2)(a) ISA or s. 4(2)(a) ISA) will amount to a criminal office. Conviction may lead to an imprisonment for a term not exceeding two years and/or a fine (s. 10(1) OSA).

2.19 Further, a member of the Intelligence Services commits an offence if he fails to take such care, to prevent the unauthorised disclosure of any document or other article relating to security or intelligence which is in his possession by virtue of his position as a member of any of those services, as a person in his position may reasonably be expected to take. See s. 8(1) OSA, as read with s. 1(1). Conviction may lead to an imprisonment for a term not exceeding three months and/or a fine (s. 10(2) OSA).

RIPA

2.20 In general, and subject to the provisions of the Code (as to which see below), the Intelligence Services are not required to seek authorisation under RIPA in order to obtain communications or communications data from foreign intelligence agencies. However, this does not mean that RIPA is of no relevance in the present context.

2.21 In particular, not least given the safeguards and oversight mechanisms that Parliament saw fit to impose in the case of interception pursuant to a RIPA interception warrant (see §§3.71-3.144 below), and in the light of the well-established principle of domestic public law set out by the House of Lords in *Padfield v Ministry*

of Agriculture, Fisheries and Food [1968] AC 997[61], it would as a matter of domestic public law be unlawful for any of the Intelligence Services to deliberately circumvent those safeguards and mechanisms (and attempt to avoid the need to apply for an interception warrant under RIPA) by asking a foreign intelligence agency to intercept certain specified communications and disclose them to the Intelligence Services. (That is not to say that there will not be circumstances where there are legitimate reasons to ask a foreign intelligence agency to intercept particular communications, for example, where it is not technically feasible for the Intelligence Services themselves to undertake the interception in question.)

2.22 Similarly, it would as a matter of basic public law be unlawful for any of the Intelligence Services to deliberately circumvent the provisions in Chapter II of Part I of RIPA or any other domestic legislation governing the acquisition of communications data by asking a foreign intelligence agency to obtain specified communications data and disclose them to the Intelligence Services. (Again, that is not to say that there will not be circumstances where there are legitimate reasons to ask a foreign intelligence agency to obtain particular communications data, *e.g.* for reasons of technical feasibility.) Moreover, that is also the express effect of the Code, as to which see below.

The Code

2.23 Chapter 12 of the Code[62] mirrors the effect of the Disclosure, recorded in the IPT's 5 December and 6 February Judgments[63]. Chapter 12 states as follows:

> ***"12 Rules for requesting and handling unanalysed intercepted communications from a foreign government***
>
> ***Application of this chapter***

[61] The principle in *Padfield* is that a statutory discretion must be used so as to promote, and not to thwart, the policy and object of the Act. The judgment is at [***See Annex 31***].
[62] [***See Annex 10***]
[63] A judicial decision of this type can be taken into account in assessing "foreseeability" for the purposes of Art. 8(2): *Uzun v. Germany* (2011) 53 EHRR 24, at §62. So, for the avoidance of doubt, prior to the issue of the (revised) Code on 15 January 2016, the domestic law position was the same, as the result of the 5 December and 6 February judgments (***See Annexes 15 and 27***).

12.1 This chapter applies to those intercepting agencies that undertake interception under a section 8(4) warrant.

Requests for assistance other than in accordance with an international mutual assistance agreement

12.2 A request may only be made by the Intelligence Services to the government of a country or territory outside the United Kingdom for unanalysed intercepted communications (and associated communications data), otherwise than in accordance with an international mutual legal assistance agreement, if either:

- *A relevant interception warrant under the Regulation of Investigatory Powers Act 2000 ("RIPA") has already been issued by the Secretary of State, the assistance of the foreign intelligence is necessary to obtain the communications at issue because they cannot be obtained under the relevant RIPA interception warrant and it is necessary and proportionate for the Intelligence Services to obtain those communications; or*
- *Making the request for the communications at issue in the absence of a relevant RIPA interception warrant does not amount to a deliberate circumvention of RIPA or otherwise frustrate the objectives of RIPA (for example, because it is not technically feasible to obtain the communications via RIPA interception), and it is necessary and proportionate for the Intelligence Services to obtain those communications.*

12.3 A request falling within the second bullet of paragraph 12.2 may only be made in exceptional circumstances and must be considered and decided upon by the Secretary of State personally.

12.4 For these purposes a "relevant RIPA interception warrant" means one of the following: (i) a section 8(1) warrant in relation to the subject at issue; (ii) a section 8(4) warrant and an accompanying certificate which includes one or more "descriptions of intercepted material" (within the meaning of section 8(4)(b) of RIPA) covering the subject's communications, together with an appropriate section 16(3) modification (for individuals known to be within the British Islands); or (iii) a section 8(4) warrant and an accompanying certificate which includes one or more "descriptions of intercepted material" covering the subject's communications (for other individuals).

Safeguards applicable to the handling of unanalysed intercepted communications from a foreign government

12.5 If a request falling within the second bullet of paragraph 12.2 is approved by the Secretary of State other than in relation to specific selectors, any communications obtained must not be examined by the intercepting agency according to any factors as are mentioned in section 16(2)(a) and (b) of RIPA unless the Secretary of State has personally considered and approved the examination of those communications by reference to such factors[64].

12.6 Where intercepted communications content or communications data are obtained by the intercepting agencies as set out in paragraph 12.2, or are otherwise received by them from the government of a country or territory outside the UK in circumstances where the material identifies itself as the product of an interception, (except in accordance with an international mutual assistance agreement), the communications content [fn whether analysed or unanalysed] and communications data [fn whether or not those data are associated with the content of communications] must be subject to the same internal rules and safeguards as the same categories of content or data, when they are obtained directly by the intercepting agencies as a result of interception under RIPA.

12.7 All requests in the absence of a relevant RIPA interception warrant to the government of a country or territory outside the UK for unanalysed intercepted communications (and associated communications data) will be notified to the Interception of Communications Commissioner."

2.24 In sum, the effect of the Code is to confirm that, in the factual premises relevant to the Liberty proceedings (and therefore to this Application), exactly the same internal safeguards governing use, disclosure, sharing, storage and destruction apply as a matter of substance to material obtained via intelligence sharing as apply to similar material obtained through interception under Part I of RIPA.

[64] The following footnote appears within chapter 12 at this point: *"All other requests within paragraph 12.2 (whether with or without a relevant RIPA interception warrant) will be made for material to, from or about specific selectors (relating therefore to a specific individual or individuals). In these circumstances the Secretary of State will already therefore have approved the request for the specific individual(s) as set out in paragraph 12.2."*

Other safeguards

2.25 The above statutory framework is underpinned by detailed internal guidance, including in the form of "arrangements" under s. 2 of the SSA and ss. 2 and 4 of the ISA, and by a culture of compliance. The latter is reinforced by the provision of appropriate mandatory training to staff within the Intelligence Services, and by vetting procedures to ensure that staff faithfully operate within the aims, safeguards and ethos of the Intelligence Services: see Mr Farr §§51-53.

Oversight mechanisms in the Intelligence Sharing Regime

2.26 There are two principal oversight mechanisms in the Intelligence Sharing Regime: the ISC; and the IPT.

The ISC

2.27 SIS and GCHQ are responsible to the Foreign Secretary,[65] who in turn is responsible to Parliament. Similarly, the Security Service is responsible to the Home Secretary, who in turn is responsible to Parliament. In addition, the ISC plays an important part in overseeing the activities of the Intelligence Services. In particular, the ISC is the principal method by which scrutiny by Parliamentarians is brought to bear on those activities.

2.28 The ISC was established by s. 10 of the ISA. As from 25 June 2013, the statutory framework for the ISC is set out in ss. 1-4 of and Sch. 1 to the JSA. The ISC has itself welcomed these changes in the JSA, and it considers that they are "broadly in line with" those that it had previously recommended to Government and which "increase accountability" [***See Annex 32***].

[65] The Chief of the Intelligence Service and the Director of GCHQ must each make an annual report on, respectively, the work of SIS and GCHQ to the Prime Minister and the Secretary of State (see ss. 2(4) and 4(4) of the ISA). An analogous duty is imposed on the Director-General of the Security Service (see s. 2(4) of the SSA).

2.29 The ISC consists of nine members, drawn from both the House of Commons and the House of Lords. Each member is appointed by the House of Parliament from which the member is to be drawn (they must also have been nominated for membership by the Prime Minister, following consultation with the leader of the opposition). No member can be a Minister of the Crown. The Chair of the ISC is chosen by its members. See s. 1 of the JSA. The current chair is The Rt Hon Dominic Grieve QC MP, a former Attorney General. The executive branch of Government has no power to remove a member of the ISC: a member of the ISC will only vacate office if he ceases to be a member of the relevant House of Parliament, becomes a Minister of the Crown or a resolution for his removal is passed by the relevant House of Parliament. See §1(2) of Sch. 1 to the JSA.

2.30 The ISC may examine the expenditure, administration, policy and operations of each of the Intelligence Services: s. 2(1). Subject to certain limited exceptions, the Government (including each of the Intelligence Services) must make available to the ISC information that it requests in the exercise of its functions. See §§4-5 of Sch. 1 to the JSA. In practice, and where it is necessary to do so for the purposes of overseeing the full range of the activities of the Intelligence Services, the ISC is provided with all such sensitive information as it needs: see Mr Farr §71.

2.31 The ISC operates within the "ring of secrecy" which is protected by the OSA. It may therefore consider classified information, and in practice takes oral evidence from the Foreign and Home Secretaries, the Director-General of the Security Service, the Chief of SIS and the Director of GCHQ, and their staff. The ISC meets at least weekly whilst Parliament is sitting. The ISC may also hold open evidence sessions: see Mr Farr §66.

2.32 The ISC meets at least weekly whilst Parliament is sitting. It is supported by staff who have the highest level of security clearance: see Mr Farr §67. Following the extension to its statutory remit as a result of the JSA, the ISC's budget has been substantially increased: see Mr Farr §69.

2.33 The ISC must make an annual report to Parliament on the discharge of its functions (s. 3(1) of the JSA), and may make such other reports to Parliament as it considers

appropriate (s. 3(2) of the JSA). Such reports must be laid before Parliament (see s. 3(6)). They are as necessary redacted on security grounds (see ss. 3(3)-(5)), although the ISC may report redacted matters to the Prime Minister (s. 3(7)). The Government lays before Parliament any response to the reports that the ISC makes.

2.34 The ISC sets its own work programme: it may issue reports more frequently than annually and has in practice done so for the purposes of addressing specific issues relating to the work of the Intelligence Services. The ISC also monitors the Government to ensure that any recommendations it makes in its reports are acted upon: see Mr Farr §70.

The IPT

2.35 The IPT was established by s. 65(1) RIPA. Members of the IPT must either hold or have held high judicial office, or be a qualified lawyer of at least 7 years' standing (§1(1) of Sch. 3 to RIPA). The President of the IPT must hold or have held high judicial office (§2(2) of Sch. 3 to RIPA).

2.36 The IPT's jurisdiction is broad. As regards the Intelligence Sharing regime, the following aspects of the IPT's *jurisdiction* are of particular relevance. The IPT has exclusive jurisdiction to consider claims under s. 7(1)(a) HRA brought against any of the Intelligence Services or any other person in respect of any conduct, or proposed conduct, by or on behalf of any of the Intelligence Services (ss. 65(2)(a), 65(3)(a) and 65(3)(b) RIPA). The IPT may consider and determine any complaints by a person who is aggrieved by any conduct by or on behalf of any of the Intelligence Services which he believes to have taken place in relation to him, to any of his property, to any communications sent by or to him, or intended for him, or to his use of any telecommunications service or system (ss. 65(2)(b), 65(4) and 65(5)(a) RIPA). Complaints of the latter sort must be investigated and then determined "by applying the same principles as would be applied by a court on an application for judicial review" (s. 67(3) RIPA).

2.37 Thus the IPT has jurisdiction to consider any claim against any of the Intelligence Services that it has obtained information from a foreign intelligence agency in breach

of the ECHR or has disclosed information to a foreign intelligence agency in breach of the ECHR. Further, the IPT can entertain any other public law challenge to any such alleged obtaining or disclosure of information.

2.38 Any person, regardless of nationality, may bring a claim in the IPT[66] As a result, the IPT is perhaps one of the most far-reaching systems of judicial oversight over intelligence matters in the world.

2.39 Pursuant to s. 68(2) RIPA, the IPT has a broad power to require a relevant Commissioner (as defined in s. 68(8)) to provide it with assistance. Thus, in the case of a claim of the type identified in §3.48 above, the IPT may require the Intelligence Services Commissioner (see ss. 59-60 of RIPA) to provide it with assistance.

2.40 S. 68(6) RIPA imposes a broad duty of disclosure to the IPT on, among others, every person holding office under the Crown.

2.41 Subject to any provision in its rules, the IPT may - at the conclusion of a claim - make any such award of compensation or other order as it thinks fit, including, but not limited to, an order requiring the destruction of any records of information which are held by any public authority in relation to any person, and an order for the quashing of a warrant: see s. 67(7) RIPA.

2. The s. 8(4) Regime

2.42 The s. 8(4) Regime is principally contained in Chapter I of Part I of RIPA and the Code, as elucidated in the IPT's 5 December Judgment[67], and the Commissioner's 2013 Annual Report. The s. 8(4) regime also incorporates aspects of the Intelligence Sharing regime addressed above.

[66] However the IPT may refuse to entertain a claim that is frivolous or vexatious (see s. 67(4)). There is also a 1 year limitation period (subject to extension where that is "equitable"): see s. 67(5) of RIPA and s. 7(5) of the HRA. Any claims under the HRA would also have to satisfy the Article 1 ECHR jurisdiction threshold.

[67] A judicial decision of this type can be taken into account in assessing "foreseeability" for the purposes of Art. 8(2): *Uzun v. Germany*, app. 35623/05, ECHR 2010, at §62.

2.43 Section 71 RIPA imposes a duty on the Secretary of State to issue, following appropriate consultation, one or more codes of practice relating to the exercise and performance of the powers and duties conferred or imposed by or under Part I of RIPA (which includes ss. 1-19). Any person exercising or performing any power or duty under ss. 1-19 must have regard to any relevant provisions of every code of practice for the time being in force: s. 72(1). Further, where the provision of a code of practice appears to the Tribunal, a court or any other tribunal to be relevant to any question arising in the proceedings, in relation to a time when it was in force, that provision of the code must be taken account in determining that question. A similar duty is imposed on the Commissioner: see s. 72(4) RIPA. The code of practice can be taken into account in assessing "foreseeability" for the purposes of Art. 8(2): *Kennedy*, at §157. The current code of practice ("the Code") was issued on 15 January 2016[68]. The previous version was issued in July 2002 ("the 2002 Code"[69]).

The interception of communications under RIPA

2.44 S. 2 RIPA provides a detailed definition of the concept of "interception":

(1) By s. 2(2), interception occurs if (among other things) a person "modifies or interferes with" a telecommunications system so as to make "available" the content of a communication which is being transmitted on that system "to a person other than the sender or intended recipient of the communication". By s. 2(1), the term "telecommunications system" means: "... *any system (including the apparatus comprised in it) which exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy*."

(2) By s. 2(6), the "modification" of a telecommunications system includes "*the attachment of any apparatus to, or other modification of or interference with ... any part of the system*". Significantly, by s. 2(8):

"For the purposes of this section the cases in which any contents of a communication are to be taken to be made available to a person while being transmitted shall include

[68] [***See Annex 10)***]
[69] [***See Annex 33***]

any case in which any of the contents of the communication, while being transmitted, are diverted or recorded so as to be available to a person subsequently."

In other words, "interception" can merely comprise the obtaining and recording of the contents of a communication (as it is being transmitted) so as to make it "available" subsequently to be read, looked at or listened by a person. No-one in fact needs to have actually read, looked at or listened to the communication for interception to occur.

2.45 Under s. 1(1) RIPA it is an offence, punishable by a term of imprisonment of up to two years and a fine,[70] for a person intentionally and without lawful authority to intercept, at any place in the UK, any communication in the course of its transmission by means of a public telecommunications system. The Commissioner also has power to serve a monetary penalty notice (of up to £50,000) on a person who has intercepted a communication without lawful authority (in circumstances which do not amount to an offence under s. 1(1)), and who was not making an attempt to act in accordance with a warrant (see s. 1(1A)).

2.46 Conduct has lawful authority for the purposes of s. 1 if it takes place in accordance with a warrant under s. 5 RIPA: s. 1(5)(b). As in RIPA itself, such warrants will be referred to as "interception warrants".

The issuing of interception warrants

2.47 Interception warrants are issued by the Secretary of State under s. 5(1) RIPA. Such warrants must be authorised personally by the Secretary of State: s. 7 RIPA.

2.48 An application must be made before an interception warrant can be issued: s. 6(1) RIPA. Such an application may only be made by or on behalf of one of the persons listed in s. 6(2) RIPA (which list includes the Director-General of the Security Service, the Chief of SIS and the Director of GCHQ). The application must contain all the detailed matters set out in §6.10 of the Code[71] (and the position was exactly the same

[70] See s. 1(7).

[71] That is: (i) the background to the operation in question, including a description of the communications to be intercepted, details of the CSP(s) and an assessment of the feasibility of the operation where it is relevant, and a description of the conduct to be authorised; (ii) the certificate

under §5.2 of the 2002 Code). This ensures that the Secretary of State has the information he needs properly to determine, under the statutory tests, whether to issue an interception warrant. The Commissioner has confirmed that:

> *"... the paperwork is almost always compliant and of a high quality. If there are occasional technical lapses, these are almost always ironed out in the interception agencies themselves or in the Secretary of State's department before the application reaches the relevant Secretary of State."* (2013 Annual Report at §3.39[72])

2.49 By s. 5(2) RIPA, the Secretary of State may not issue an interception warrant unless he believes:

> *"(a) that the warrant is necessary on grounds falling within subsection (3); and*
> *(b) that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct."*

2.50 When considering whether the requirements of s. 5(2) are satisfied, the Secretary of State must take into account "*whether the information which it is thought necessary to obtain under the warrant could reasonably be obtained by other means*": see s. 5(4) RIPA.

2.51 The nature of the proportionality assessment that the Secretary of State should undertake before issuing a warrant is further expanded upon in §§3.6-3.7 of the Code. In particular, §3.7 of the Code explains that the following elements of proportionality should be considered:

> *"- balancing the size and scope of the proposed interference against what is sought to be achieved;*
> *- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;*

---

that will regulate the examination of intercepted material; (iii) an explanation of why the interception is considered to be necessary for one or more of the s.5(3) purposes; (iv) a consideration of why the conduct to be authorised by the warrant is proportionate to what is sought to be achieved by that conduct; (v) where an application is urgent, supporting justification; (vi) an assurance that intercepted material will be read, looked at or listened to only so far as it is certified and it meets the conditions of ss.16(2)-(6) RIPA; and (vii) an assurance that all material intercepted will be handled in accordance with the safeguards required by ss.15 and 16 RIPA.

[72] ***[See Annex 11]***

-considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result; and

-evidencing, as far as reasonably practicable, what other methods have been considered and were either not implemented or have been employed but which are assessed as insufficient to fulfil operational objectives without the addition of the intercept material sought."

(Broadly equivalent provisions were equally contained in §§2.4-2.5 of the 2002 Code.)

2.52 A warrant is necessary on grounds falling within s. 5(3) only if it is necessary (a) in the interests of national security, (b) for the purpose of preventing or detecting[73] serious crime[74] or (c) for the purpose of safeguarding the economic well-being of the UK, in circumstances appearing to the Secretary of State to be relevant to the interests of national security.

2.53 The words "in circumstances appearing to the Secretary of State to be relevant to the interests of national security", which narrow purpose (c), were added to s.5(3) RIPA by the Data Retention and Investigatory Powers Act 2014 ("DRIPA") (See Annex 34), with effect from 17 July 2014. However, even prior to 17 July 2014, the 2002 Code similarly narrowed purpose (c) as regarded the s.8(4) Regime[75]. The Code states (and the 2002 Code stated) that the Secretary of State must consider whether the economic well-being of the UK which is to be safeguarded is, on the facts of the case, directly related to national security, and the Secretary of State cannot issue a warrant on s. 5(3)(c) grounds unless such a "*direct link*" has been established: see Code, §6.12.

2.54 A further limitation on purpose (c) is provided by s. 5(5) RIPA:

"A warrant shall not be considered necessary [for the purpose of safeguarding the economic well-being of the United Kingdom, in circumstances appearing to the Secretary of State to be relevant to the interests of national security] unless the

[73] The terms "preventing" and "detecting" are defined in s. 81(5) of RIPA.
[74] The term "serious crime" is defined in ss. 81(2)(b) and 81(3) of RIPA.
[75] This was the case under §5.4 of the Code in the version from July 2002. See now §6.12 of the Code.

information which it is thought necessary to obtain is information relating to the acts or intentions of persons outside the British Islands."

2.55 The Commissioner has confirmed that the Secretaries of State provide a real and practical safeguard:

> *"The Secretaries of State themselves are entirely conscientious in undertaking their RIPA 2000 Part I Chapter I duties. They do not rubber stamp applications. On the contrary, they sometimes reject applications or require more information."* [*2013 Annual Report at §3.40*]

2.56 Further, as regards s. 8(4) warrants in particular, the Commissioner found in §6.5.43 of his 2013 Annual Report:

> "• *the Secretaries of State who sign warrants and give certificates are well familiar with the process; well able to judge by means of the written applications whether to grant or refuse the necessary permissions; and well supported by experienced senior officials who are independent from the interception agencies making the applications;*
> • *if a warrant is up for renewal, the Secretary of State is informed in writing of the intelligence use the interception warrant has produced in the preceding period. Certificates are regularly reviewed and subject to modification by the Secretary of State ...."*

2.57 All warrant applications under the s. 8(4) regime must be kept so that they can be scrutinised by the Commissioner: §6.27 of the Code (and to similar effect, §5.17 of the 2002 Code).

Section 8(4) warrants

2.58 The contents of interception warrants are dealt with under s. 8 RIPA. Provision is made for two types of warrant. The type of warrant of relevance in the present case - a s. 8(4) warrant - is provided for in s. 8(4)-(6):

> *"(4) Subsections (1) and (2)[76] shall not apply to an interception warrant if-*
>
> *(a) the description of communications to which the warrant relates confines the conduct authorised or required by the warrant to conduct falling within subsection (5); and*
>
> *(b) at the time of the issue of the warrant, a certificate applicable to the warrant has been issued by the Secretary of State certifying-*
>
> *(i) the descriptions of intercepted material[77] the examination of which he considers necessary; and*
>
> *(ii) that he considers the examination of material of those descriptions necessary as mentioned in section 5(3)(a), (b) or (c).*
>
> *(5) Conduct falls within this subsection if it consists in-*
>
> *(a) the interception of external communications in the course of their transmission by means of a telecommunication system; and*
>
> *(b) any conduct authorised in relation to any such interception by section 5(6).*
>
> *(6) A certificate for the purposes of subsection (4) shall not be issued except under the hand of the Secretary of State."*

2.59 The term "*communication*" is defined broadly in s. 81(1) RIPA to include (among other things) "*anything comprising speech, music, sounds, visual images or data of any description*". The term "*external communication*" is defined in s. 20 to mean "*a communication sent or received outside the British islands*". In addition, §6.5 of the Code provides (and §5.1 of the 2002 Code was to similar effect):

> *"External communications are defined by RIPA to be those which are sent or received outside the British Islands. They include those which are both sent and received outside the British Islands, whether or not they pass through the British Islands in course of their transmission. They do not include communications both sent and received in the British Islands, even if they pass outside the British Islands en route. For example, an email from a person in London to a person in Birmingham will be an internal, not an external, communication for the purposes of section 20 of RIPA, whether or not it is routed via IP addresses outside the British Islands, because both the sender and intended recipient are within the British*

[76] See §2.68 below.
[77] Defined in s. 20 to mean, in relation to an interception warrant, "the contents of any communications intercepted by an interception to which the warrant relates".

Islands."

2.60 By s. 5(1), a warrant may authorise or require:

> "*... the person to whom it is addressed, by any such conduct as may be described in the warrant, to secure any one or more of the following –*
>
> *(a) the interception in the course of their transmission by means of a postal service or telecommunication system of the communications described in the warrant ...*"

2.61 Further, s. 5(6) provides in relevant part:

> "*The conduct authorised by an interception warrant shall be taken to include –*
>
> *(a) all such conduct (including the interception of communications not identified by the warrant) as it is necessary to undertake in order to do what is expressly authorised or required by the warrant;*
>
> *(b) conduct for obtaining related communications data*[78]*;...*"

2.62 The reference in s. 5(6)(a) to "*communications*" as opposed to "*external communications*" is to be noted. In particular, s. 5(6)(a) makes clear that the conduct authorised by a s. 8(4) warrant may in principle include the interception of internal communications insofar as that is necessary in order to intercept the external communications to which the warrant relates.

2.63 When the Secretary of State issues a s.8(4) warrant, it must be accompanied by a certificate in which the Secretary of State describes the intercepted material that may be examined, and certifies that he considers examination of that material to be necessary for one or more of the purposes in s.5(3) RIPA: see s.8(4)(b) RIPA and §6.14 of the Code. The Code further states at §6.14[79]:

[78] "Related communications data", in relation to a communication intercepted in the course of transmission by means of a telecommunication system, is defined to be so much of any communications data as (a) is obtained by, or in connection with, the interception; and (b) relates to the communication. See s. 20 of RIPA.

[79] See also §6.3 of the 2002 Code.

> *"The purpose of the statutory certificate is to ensure that a selection process is applied to intercepted material so that only material described in the certificate is made available for human examination. Any certificate must broadly reflect the "Priorities for Intelligence Collection" set by the NSC for the guidance of the intelligence agencies. For example, a certificate might provide for the examination of material providing intelligence on terrorism (as defined in the Terrorism Act 2000) or on controlled drugs (as defined by the Misuse of Drugs Act 1971). The Interception of Communications Commissioner must review any changes to the descriptions of material specified in a certificate."*

2.64 The Code states at §6.7:

> *"When conducting interception under a section 8(4) warrant, an intercepting agency must use its knowledge of the way in which international communications are routed, combined with regular surveys of relevant communication links, to identify those individual communications bearers that are most likely to contain external communications that will meet the descriptions of material certified by the Secretary of State under section 8(4). It must also conduct the interception in ways that limit the collection of non-external communications to the minimum level compatible with the objective of intercepting wanted external communications."*

2.65 The s. 8(4) regime does not impose any express limit on the number of external communications which may fall within "*the description of communications to which the warrant relates*" in s. 8(4)(a). So in principle, it authorises the interception of all communications passing down a bearer or bearers.

2.66 The s. 8(4) regime does not seek to limit the type of communications at issue for the purposes of s. 8(5)(a), save for the requirement that they be "*external*". Thus the broad definition of "*communication*" in s. 81 applies and, in principle, anything that falls within that definition may fall within s.8(5)(a) insofar as it is "*external*".

2.67 Like all applications for s. 8(4) warrants, the warrants themselves (and their accompanying certificates) must be kept so as to be available to be scrutinised by the Commissioner: see §6.27 of the Code (and, to similar effect, §5.17 of the 2002 Code).

2.68 The other type of interception warrant - the s. 8(1) warrant - should also be noted. A s. 8(1) warrant conforms to the requirements of s. 8(1)-(3) of RIPA:

> "*(1) An interception warrant must name or describe either-*
>
> *(a) one person as the interception subject; or*
>
> *(b) a single set of premises as the premises in relation to which the interception to which the warrant relates is to take place.*
>
> *(2) The provisions of an interception warrant describing communications the interception of which is authorised or required by the warrant must comprise one or more schedules setting out the addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying the communications that may be or are to be intercepted.*
>
> *(3) Any factor or combination of factors set out in accordance with subsection (2) must be one that identifies communications which are likely to be or to include-*
>
> *(a) communications from, or intended for, the person named or described in the warrant in accordance with subsection (1); or*
>
> *(b) communications originating on, or intended for transmission to, the premises so named or described.*"

Processing the intercepted communications to obtain communications that can be read, looked at or listened to

2.69 By s. 15(1)(b) RIPA, the Secretary of State is under a duty to ensure, in relation to s. 8(4) warrants, that such arrangements are in force as he considers necessary for securing that the requirements of s. 16 are satisfied.

2.70 Section 16(1) imposes the requirement that:

> "*…the intercepted material is read, looked at or listened to by the persons to whom it becomes available by virtue of the warrant to the extent only that it-*

(a) has been certified as material the examination of which is necessary as mentioned in section 5(3)(a), (b) or (c); and

(b) falls within subsection (2)."

2.71 Given the definition of "intercepted material", s. 16(1) applies both to external communications and to any internal communications that may have been intercepted under a s. 8(4) warrant[80].

2.72 The Code expands upon the requirement in s.16(1) that before intercepted material is examined, it must have been certified as necessary to examine it for one of the statutory purposes in s.5(3) RIPA: see Code, §6.14, and §3.76 above.

2.73 The Commissioner must review any changes to the descriptions of material specified in a certificate: see Code, §6.14.

2.74 Section 16(2) provides in relevant part:

"*…intercepted material falls within this subsection so far only as it is selected to be read, looked at or listened to otherwise than according to a factor which-*

(a) is referable to an individual who is known to be for the time being in the British Islands; and

(b) has as its purpose, or one of its purposes, the identification of material contained in communications sent by him, or intended for him."

2.75 Section 16(2) is subject to ss. 16(3) and 16(4), which provide for strictly limited circumstances in which it is permissible to select intercepted material by reference to factors which satisfy ss. 16(2)(a) and 16(2)(b). In particular, section 16(3) states:

"*(3) Intercepted material falls within subsection (2), notwithstanding that it is selected by reference to any such factor as is mentioned in paragraph (a) and (b) of*

[80] Section 20 RIPA defines "intercepted material", in relation to an interception warrant, as *"the contents of any communications intercepted by an interception to which the warrant relates"*. Thus, it includes internal as well as external communications intercepted pursuant to the warrant.

that subsection, if-

(a) It is certified by the Secretary of State for the purposes of section 8(4) that the examination of material selected according to factors referable to the individual in question is necessary as mentioned in subsection 5(3)(a), (b) or (c); and

(b) The material only relates only to communications sent during a period specified in the certificate that it no longer than the permitted maximum[81]*."*

2.76 In addition, pursuant to s. 6(1) HRA, the selection of any particular intercepted material to be read, looked at or listened to must always be proportionate, having regard to the particular circumstances, for Art. 8(2) purposes.

2.77 Thus, the s. 8(4) regime envisages the following (which is also explained in the Code at §6.1, entitled "Section 8(4) interception in practice"[82]):

(1) A volume of intercepted material will be generated by the act of interception pursuant to a s. 8(4) warrant. The volume may in principle be substantial. Further, the intercepted material may be recorded so as to be available for subsequent examination (see s. 2(8) of RIPA).

(2) Pursuant to the s. 16 arrangements, a much smaller volume of intercepted material is then selected to be read, looked at or listened to by persons. The intercepted material so selected must be certified (in the Secretary of State's certificate) as material of a description that may be examined, and as material the examination of which is necessary as mentioned in s. 5(3)(a), (b) or (c) of

---

[81] The "permitted maximum" is either 3 or 6 months, depending upon whether the examination of the material is certified as necessary in the interests of national security: see section 16(3A) RIPA.

[82] §6.4 of the Code states:
"A section 8(4) warrant authorises the interception of external communications. Where a section 8(4) warrant results in the acquisition of large volumes of communications, the intercepting agency will ordinarily apply a filtering process to automatically discard communications that are unlikely to be of intelligence value. Authorised persons within the intercepting agency may then apply search criteria to select communications that are likely to be of intelligence value in accordance with the terms of the Secretary of State's certificate. Before a particular communication may be accessed by an authorised person within the intercepting agency, the person must provide an explanation of why it is necessary for one of the reasons set out in the certificate accompanying the warrant issued by the Secretary of State, and why it is proportionate in the particular circumstances. This process is subject to internal audit and external oversight by the Interception of Communications Commissioner. Where the Secretary of State is satisfied that it is necessary, he or she may authorise the selection of communications of an individual who is known to be in the British Islands. In the absence of such an authorisation, an authorised person must not select such communications."

RIPA (*i.e.* in interests of national security, for the purpose of preventing or detecting serious crime or for the purpose of safeguarding the economic well-being of the United Kingdom, in circumstances appearing to the Secretary of State to be relevant to the interests of national security). In other words, the certificate regulates the examination of the intercepted material (see §6.14 of the Code). In addition, any individual selection of intercepted material must be proportionate in the particular circumstances (given s. 6(1) HRA, and see §§3.6-3.7 of the Code). Further, provision is made in s. 16 RIPA to limit the extent to which intercepted material can be selected by reference to "factors" that in essence would select communications to or from an individual who is known to be (at the time) in the British Islands. The Commissioner has confirmed that the s. 8(4) regime does not authorise indiscriminate trawling (see the 2013 Annual Report at §6.5.43 [***See Annex 11***]).

(3) Insofar as the intercepted material may not be proportionately selected to be read, looked at or listened to in accordance with the certificate and pursuant to s. 16 of RIPA and s. 6(1) of the HRA, then it cannot be read, looked at or listened to by anyone.

2.78 It is thus necessary and important to distinguish between the act of interception in and of itself; and a person actually reading, looking at or listening to intercepted material. That is the distinction which the misleading characterisation of the s.8(4) Regime as entailing "mass surveillance" consistently fails to recognise.

2.79 Further detail of the s.16 arrangements is set out in the Code at §§7.14-7.19:

"7.14 In general, automated systems must, where technically possible, be used to effect the selection in accordance with section 16(1) of RIPA. As an exception, a certificate may permit intercepted material to be accessed by a limited number of specifically authorised staff without having been processed or filtered by the automated systems. Such access may only be permitted to the extent necessary to determine whether the material falls within the main categories to be selected under the certificate, or to ensure that the methodology being used remains up to date and effective. Such checking must itself be necessary on the grounds specified in section 5(3) of RIPA. Once those functions have been fulfilled, any copies made of the

material for those purposes must be destroyed in accordance with section 15(3) of RIPA. Such checking by officials should be kept to an absolute minimum; whenever possible, automated selection techniques should be used instead. Checking will be kept under review by the Interception of Communications Commissioner during his or her inspections.

7.15 Material gathered under a section 8(4) warrant should be read, looked at or listened to only by authorised persons who receive regular mandatory training regarding the provisions of RIPA and specifically the operation of section 16 and the requirements of necessity and proportionality. These requirements and procedures must be set out in internal guidance provided to all authorised persons and the attention of all authorised persons must be specifically directed to the statutory safeguards. All authorised persons must be appropriately vetted (see paragraph 7.10 for further information).

7.16 Prior to an authorised person being able to read, look at or listen to material, a record should be created setting out why access to the material is required consistent with, and pursuant to, section 16 and the applicable certificate, and why such access is proportionate. Save where the material or automated systems are being checked as described in paragraph 7.14, the record must indicate, by reference to specific factors, the material to which access is being sought and systems should, to the extent possible, prevent access to the material unless such a record has been created. The record should include any circumstances that are likely to give rise to a degree of collateral infringement of privacy, and any measures taken to reduce the extent of the collateral intrusion. All records must be retained for the purposes of subsequent examination or audit.

7.17 Access to the material as described in paragraph 7.15 must be limited to a defined period of time, although access may be renewed. If access is renewed, the record must be updated with the reason for the renewal. Systems must be in place to ensure that if a request for renewal is not made within that period, then no further access will be granted. When access to the material is no longer sought, the reason for this must also be explained in the record.

7.18 Periodic audits should be carried out to ensure that the requirements set out in

section 16 of RIPA and Chapter 3 of this code are being met. These audits must include checks to ensure that the records requesting access to material to be read, looked at or listened to have been correctly compiled, and specifically, that the material requested falls within the matters certified by the Secretary of State. Any mistakes or procedural deficiencies should be notified to management, and remedial measures undertaken. Any serious deficiencies should be brought to the attention of senior management and any breaches of safeguards (as noted in paragraph 7.1) must be reported to the Interception of Communications Commissioner. All intelligence reports generated by the authorised persons must be subject to a quality control audit.

7.19 In order to meet the requirements of RIPA described in paragraph 6.3 above, where a selection factor refers to an individual known to be for the time being in the British Islands, and has as its purpose or one of its purposes, the identification of material contained in communications sent by or intended for him or her, a submission must be made to the Secretary of State, or to a senior official in an urgent case, giving an explanation of why an amendment to the section 8(4) certificate in relation to such an individual is necessary for a purpose falling within section 5(3) of RIPA and is proportionate in relation to any conduct authorised under section 8(4) of RIPA."

2.80 Although the full details of the s. 16 arrangements cannot be made public (Mr Farr §100), records must be kept of them, and they must be made available to the Commissioner (§§6.28 and 7.1 of the Code[83]), who is required to keep them under review (see s. 57(2)(d)(i) of RIPA). Any breach of the arrangements must be reported to the Commissioner (§7.1 of the Code[84]). Further, if the Commissioner considers that the arrangements have proved inadequate in any relevant respect he must report this to the Prime Minister (see s. 58(3)).

2.81 The Commissioner's advice and approval was sought and given in respect of the documents constituting the s. 16 arrangements either before or shortly after 2 October 2000 (when RIPA came into force): §15 of the Commissioner's Annual Report for 2000 (See Annex 35). In practice, the advice of the Commissioner is sought when any substantive change is proposed to the arrangements.

[83] See also to similar effect §5.17 of the 2002 Code.
[84] See also to similar effect §6.1 of the 2002 Code.

The duration, cancellation, renewal and modification of warrants and certificates under RIPA

2.82 A s. 8(4) warrant ceases to have effect at the end of the "relevant period", unless it is renewed by an instrument under the hand of the Secretary of State: s. 9(1) RIPA. The "relevant period" for a s. 8(4) warrant is, depending on the circumstances, either three or six months (see s. 9(6)).

2.83 A section 8(4) warrant may be renewed at any point before its expiry date. The application for renewal must be made to the Secretary of State, and must contain all the detailed information set out in §6.10 of the Code, just as with the original warrant application (see §6.22 of the Code[85]). The Code states at §6.22 with regard to the renewal application:

> *"…the applicant must give an assessment of the value of interception to date and explain why it is considered that interception continues to be necessary for one or more of the statutory purposes in section 5(3), and why it is considered that interception continues to be proportionate."*

2.84 No s. 8(4) warrant may be renewed unless the Secretary of State believes that the warrant continues to be necessary on grounds falling within s. 5(3) RIPA: s. 9(2). Further, by s. 9(3), the Secretary of State must cancel a s. 8(4) warrant if he is satisfied that the warrant is no longer necessary on grounds falling within s. 5(3). Detailed provision is made for the modification of warrants and certificates by s. 10 RIPA.

2.85 §6.27 of the Code requires records to be kept of copies of all renewals and modifications of s. 8(4) warrants / certificates, and the dates on which interception is started and stopped (and §5.17 of the 2002 Code was to like effect).

The handling and use of intercepted material and related communications data

[85] See also to parallel effect §5.12 of the 2002 Code.

2.86 Section 15(1)(a) RIPA imposes a duty on the Secretary of State to ensure, in relation to s. 8(4) warrants (and s. 8(1) warrants), that such arrangements are in force as he considers necessary for securing that the requirements of ss. 15(2) and 15(3) are satisfied in relation to the intercepted material and any related communications data.[86] As regards material intercepted under the s. 8(4) regime, the requirements in ss. 15(2) and 15(3) apply both to intercepted material that may be read, looked at or listened to pursuant to s. 16 RIPA and the certificate in question (and s. 6(1) HRA) and to material that may not be so examined. Further, given the definition of "intercepted material", it is clear that ss. 15(2) and 15(3) apply both to external communications and to any internal communications that may also have been intercepted under a s. 8(4) warrant.

2.87 In relation to intercepted material and any related communications data, the requirements of s. 15(2) are that:

> "*(a) the number of persons to whom any of the material or data is disclosed or otherwise made available,*
> *(b) the extent to which any of the material or data is disclosed or otherwise made available,*
> *(c) the extent to which any of the material or data is copied, and*
> *(d) the number of copies that are made,*
> *is limited to the minimum that is necessary for the authorised purposes*."

2.88 The authorised purposes include those set out in s. 5(3), facilitating the carrying out of the functions of the Commissioner or the IPT and ensuring that a person conducting a criminal prosecution has the information he needs to determine what is required of him by his duty to secure the fairness of the prosecution: see s. 15(4).

2.89 By s. 15(5) RIPA, the s. 15(2) arrangements must include such arrangements as the Secretary of State considers necessary for securing that every copy of the material / data is stored, for so long as it is retained, in a secure manner.[87]

[86] This duty is subject to s. 15(6) (see §2.99 below).
[87] The seventh data protection principle imposes a similar obligation, insofar as the intercepted material amounts to personal data.

2.90 In relation to intercepted material and any related communications data, the requirements of s. 15(3) are that:

> *"…each copy of the material or data (if not destroyed earlier) is destroyed as soon as there are no longer any grounds for retaining it as necessary for any of the authorised purposes."*[88]

The term "copy" is defined widely for the purposes of s. 15. In particular, s. 15(8) provides:

> *"In this section 'copy', in relation to intercepted material or related communications data, means any of the following (whether or not in documentary form)-*
>
> *(a) any copy, extract or summary of the material or data which identifies itself as the product of an interception, and*
>
> *(b) any record referring to an interception which is a record of the identities of the persons to or by whom the intercepted material was sent, or to whom the communications data relates,*
>
> *and 'copied' shall be construed accordingly."*

2.91 Chapter 7 of the Code expands on the nature of these safeguards. It begins by emphasising at §7.1 that all material intercepted under a s. 8(4) warrant (including related communications data) must be handled in accordance with the safeguards that the Secretary of State has approved under section 15.

2.92 The Code then provides further information about the s. 15 safeguards, including information about safeguards on disclosure to foreign states. As regards the dissemination of intercepted material and any related communications data, §7.3-7.5 provide[89]:

[88] Insofar as intercepted material amounts to personal data, the same obligation is in substance also imposed by virtue of the fifth data protection principle.

[89] See also §§6.4-6.6 of the 2002 Code.

"7.3 The number of persons to whom any of the intercepted material[90] is disclosed, and the extent of disclosure, must be limited to the minimum that is necessary for the authorised purposes set out in section 15(4) of RIPA. This obligation applies equally to disclosure to additional persons within an agency, and to disclosure outside the agency.[91] It is enforced by prohibiting disclosure to persons who do not hold the required security clearance, and also by the need-to-know principle: intercepted material must not be disclosed to any person unless that person's duties, which must relate to one of the authorised purposes, are such that he needs to know about the material to carry out those duties.[92] In the same way only so much of the material may be disclosed as the recipient needs. For example if a summary of the material will suffice, no more than that should be disclosed.

7.4 The obligations apply not just to the original interceptor, but also to anyone to whom the material is subsequently disclosed. In some cases this will be achieved by requiring the latter to obtain the originator's permission before disclosing the material further. In others, explicit safeguards are applied to secondary recipients.

7.5 Where intercepted material is disclosed to the authorities of a country or territory outside the UK, the agency must take reasonable steps to ensure that the authorities in question have and will maintain the necessary procedures to safeguard the intercepted material, and to ensure that it is disclosed, copied, distributed and retained only to the minimum extent necessary. In particular, the intercepted material must not be further disclosed to the authorities of a third country or territory unless explicitly agreed with the issuing agency, and must be returned to the issuing agency or securely destroyed when no longer needed."

2.93 Further, as §7.10 of the Code makes clear, arrangements regarding personnel security impose strict limits on who may gain access to intercepted material and any related communications data[93]:

[90] It is apparent from the drafting of §7.1 of the Code that references in Chapter 6 to "the material" and "the intercepted material" are to the material intercepted under an interception warrant, including any related communications data, and that therefore those terms do not bear the technical meaning given to them in s. 20 of RIPA.

[91] This aspect of the Code makes clear that intercepted material may be disclosed to other public authorities.

[92] Thus, for instance, if GCHQ intercepted the communication of a terrorist suspect of interest to an intelligence officer that revealed that the terrorist suspect was planning to travel to London but also that the suspect's cousin was shortly to become a father, then only the former part of the communication would be disclosed to the intelligence officer.

[93] See also to parallel effect §6.9 of the 2002 Code.

> "*All persons who may have access to intercepted material or need to see any reporting in relation to it must be appropriately vetted. On an annual basis, managers must identify any concerns that may lead to the vetting of individual members of staff being reconsidered. The vetting of each individual member of staff must also be periodically reviewed. Where it is necessary for an officer of one agency to disclose intercepted material to another, it is the former's responsibility to ensure that the recipient has the necessary clearance.*"

2.94 The Government's policy on security vetting was announced to Parliament by the then Prime Minister in 1994. The policy was most recently set out in a Cabinet Office booklet, "*HMG Personnel Security Controls*" (***See Annex 36***). In practice, the policy ensures that those who may have access to intercepted material and any related communications data have been rigorously vetted.

2.95 §7.6 of the Code explains the restrictions and safeguards that apply to copying[94]:

> "*Intercepted material may only be copied to the extent necessary for the authorised purposes set out in section 15(4) of RIPA. Copies include not only direct copies of the whole of the material, but also extracts and summaries which identify themselves as the product of interception, and any record referring to an interception which is a record of the identities of the persons to or by whom the intercepted material was sent. The restrictions are implemented by requiring special treatment of such copies, extracts and summaries that are made by recording their making, distribution and destruction.*"

2.96 The safeguards in relation to storage and destruction are addressed in §§7.7 and 7.8-7.9 of the Code[95] respectively:

> "*7.7 Intercepted material, and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss or theft. It must be held so as to be inaccessible to persons without the required level of vetting. This*

[94] §6.6 of the 2002 Code was to exactly the same effect.
[95] See also §§6.7-6.8 of the 2002 Code, which contained the same provisions as §§7.7-7.8 of the Code.

requirement to store intercept product securely applies to all those who are responsible for the handling of this material, including [communications service providers]....
material

7.8 Intercepted, and all copies, extracts and summaries which can be identified as the product of an interception, must be securely destroyed as soon as it is no longer needed for any of the authorised purposes. If such material is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid under section 15(3) of RIPA.

7.9 Where an intercepting agency undertakes interception under a section 8(4) warrant and receives unanalysed intercepted material and related communications data from interception under that warrant, the agency must specify (or must determine on a system by system basis) maximum retention periods for different categories of the data which reflect its nature and intrusiveness. The specified periods should normally be no longer than two years, and should be agreed with the Interception of Communications Commissioner. Data may only be retained for longer than the applicable maximum retention periods if prior authorisation is obtained from a senior official within the particular intercepting agency on the basis that continued retention of the data has been assessed to be necessary and proportionate. If continued retention of any such data is thereafter assessed to no longer meet the tests of necessity and proportionality, it must be deleted. So far as possible, all retention periods should be implemented by a process of automated deletion, which is triggered once the applicable maximum retention period has been reached for the data at issue.[96]"

2.97 Although the full details of the s. 15 safeguards cannot be made public [Mr Farr *§100*], they are made available to the Commissioner (§7.1 of the Code[97]) who is required to keep them under review (see s. 57(2)(d)(i) RIPA). Further, to facilitate oversight by the Commissioner, each intercepting agency is required to keep a record of the arrangements for meeting the requirements of sections 15(2) and (3) RIPA (see

[96] §7.9 has been added in the new version of the Code (i.e. the version from January 2016) to reflect the Disclosure in the Liberty proceedings.
[97] And see, to the same effect, §6.1 of the 2002 Code.

§6.28 of the Code). Any breach of the arrangements must be reported to the Commissioner (§7.1 of the Code), and if the Commissioner considers that the arrangements have proved inadequate in any relevant respect he must report this to the Prime Minister (see s. 58(3) RIPA).

2.98 The Commissioner's advice and approval was sought and given in respect of the documents constituting the s. 15 arrangements either before or shortly after 2 October 2000 (when RIPA came into force): §15 of the Commissioner's 2000 Annual Report 2000 [***See Annex 35***]. In practice, the advice of the Commissioner is sought when any substantive change is proposed to the s. 15 arrangements that apply under the s. 8(4) regime [*Farr §104*].

2.99 For completeness, s. 15(6) RIPA is to be noted.

> "*Arrangements in relation to interception warrants which are made for the purposes of subsection (1) –*
>
> *(a) shall not be required to secure that the requirements of subsections (2) and (3) are satisfied in so far as they relate to any of the intercepted material or related communications data, or any copy of any such material or data, possession of which has been surrendered to any authorities of a country or territory outside the United Kingdom; ...*"

Instead, the s. 15(1) arrangements must secure that possession of the intercepted material and data (or copies thereof) is only surrendered to authorities of a country or territory outside the United Kingdom if it appears to the Secretary of State that requirements corresponding to those in ss. 15(2)-(3) will apply, to such extent (if any) as the Secretary of State thinks fit and that, in effect, appropriate restrictions are in place as regards the potential use of any of the intercepted material in proceedings outside the United Kingdom. See s. 15(6)(b) and s. 15(7). As the explanatory notes make clear, ss. 15(6)-(7) apply to the surrendering of communications / communications data pursuant to an obligation under a mutual assistance agreement. They do not apply to the discretionary disclosure of communications / communications data to any foreign intelligence agency under the SSA / ISA as read with s. 19 CTA and s. 6(1) HRA. Such discretionary disclosures have to comply with

the "*arrangements*" required by s. 15(2) and s. 15(3) RIPA.

2.100 The criminal law also protects the confidentiality of information obtained pursuant to an interception warrant:

(1) Where an interception warrant has been issued or renewed, s. 19(1) RIPA imposes a duty on, among others, every person holding office under the Crown to keep secret "everything" in the intercepted material, together with any related communications data. Subject to certain limited defences (including the defence under s. 19(9)(b) that the disclosure was confined to a disclosure authorised by the warrant or the person to whom the warrant is or was addressed), it is an offence for a person to make a disclosure to another of anything that he is required to keep secret under s. 19. Any disclosure of intercepted material or related communications data in breach of the s. 15 arrangements would constitute a criminal offence under s. 19 (unless, exceptionally, one of the defences in s. 19 applied). The maximum penalty for this offence is a fine and five years imprisonment. See s. 19(4) RIPA.

(2) Under s. 4(1) OSA, it is a criminal offence for a person who is or has been a Crown servant or government contractor to disclose, without lawful authority, any information, document or other article to which s. 4 OSA applies and which is or has been in his possession by virtue of his position as such. By virtue of s. 4(3)(a) OSA, s. 4 OSA applies to any information obtained under the authority of an interception warrant. A conviction under s. 4 OSA can lead to a fine or a term of imprisonment for up to two years: s. 10(1) OSA.

(3) By s. 8 OSA, it is also an offence for members of the Intelligence Services to fail to take reasonable care to prevent unauthorised disclosure of *e.g.* documents that contain intercepted material (or related communications data). See §§3.22-3.23 above.

3.42 Finally, as regards handling and use, the practical effect of s. 17 RIPA is that neither intercepted material nor any related communications data can ever be admitted in evidence in criminal trials. (The equivalent prohibition in s. 17 for civil proceedings is subject to the closed material procedure in Part 2 of the JSA.)

The practical operation of the s. 8(4) Regime

2.101 In §6.5.1 of his 2012 Annual Report, the Commissioner stated that "*GCHQ staff conduct themselves with the highest levels of integrity and legal compliance*" [***See Annex 37***]. In §6.5.2 of that report, he observed that "*officers working for SIS conduct themselves in accordance with the highest levels of ethical and legal compliance*". As regards the Security Service, §6.5.4 of the 2012 Annual Report records:

> "*I was again impressed by the attitude and expertise of the staff I met who are involved in the interception of communications and I am satisfied that they act with the highest levels of integrity.*"

2.102 To similar effect, the Commissioner concluded as follows in his 2013 Annual Report:

> "*Our inspections and investigations lead me to conclude that the Secretaries of State and the agencies that undertake interception operations under RIPA 2000 Chapter I Part I do so lawfully, conscientiously, effectively and in the national interest. This is subject to the specific errors reported and the inspection recommendations. These require attention but do not materially detract from the judgment expressed in the first sentence.*" [***See Annex 11***]

2.103 In his 2014 Annual Report (***See Annex 12***), the Commissioner indicated that he had undertaken a detailed investigation into GCHQ's [98] application of individual selection criteria from stored selected material initially derived from s.8(4) interception, reviewing the "*breadth and depth of the internal procedures for the selection of material to ensure that they were sufficiently strong in all respects*". He concluded that, although there was no pre-authorisation or authentication process to select material, and consideration should be given to whether such a process was feasible or desirable, the selection procedure "*is carefully and conscientiously undertaken both in general and, so far as we were able to judge, by the individuals themselves*", and "*random audit checks are conducted retrospectively of the justifications for selection, by or under the*

[98] The Commissioner focused upon GCHQ as "the interception agency that makes most use of section 8(4) warrants and selection criteria": see the 2014 Annual Report, §6.37.

direction of GCHQ's Internal Compliance Team, and in addition, the IT Security Team conducts technical audits to identify and further investigate any possible unauthorised use", which was *"a strong safeguard"*: see the 2014 Report, §§6.38-6.39.

2.104 The Commissioner also stated at §6.40 of the 2014 Report (***See Annex 12***):

> *"The related matters that my office investigated included the detail of a number of other security and administrative safeguards in place with GCHQ (which are not just relevant to interception work). These included the security policy framework (including staff vetting), the continuing instruction and training of all relevantly engaged staff in the legal and other requirements of the proper operation of RIPA 2000 with particular emphasis on Human Rights Act requirements, and the development and operation of computerised systems for checking and searching for potentially non-compliant use of GCHQ's systems and premises. I was impressed with the quality, clarity and extent of the training and instruction material and the fact that all staff are required to undertake and pass a periodic online test to demonstrate their continuing understanding of the legal and other requirements."*

Oversight mechanisms in the s. 8(4) regime

2.105 There are three principal oversight mechanisms in the s. 8(4) Regime:

(1) the Commissioner (see §§2.106-2.119 below);
(2) the ISC (see §§2.27-2.34 above); and
(3) the IPT (see §§2.35-2.41 above, and §§2.120-2.124 below).

The Commissioner

2.106 The Commissioner provides an important means by which the exercise by the Intelligence Services of their interception powers under RIPA may be subject to effective oversight whilst maintaining appropriate levels of confidentiality regarding those activities.

2.107 The Prime Minister is under a duty to appoint a Commissioner (see s. 57(1) RIPA). By s. 57(5), the person so appointed must hold or have held high judicial office, so as to ensure that he is appropriately independent from the Government. The Commissioner was Sir Anthony May from 31 December 2012 until 4 November 2015, when Sir Stanley Burnton was appointed. The Commissioner (quite properly) considers himself to be independent from Government and the Intelligence Services: see e.g. the 2013 Annual Report at §§6.3.1-6.3.4 (***See Annex 11***).

2.108 Under s. 57(7), the Commissioner must be provided with such technical facilities and staff as are sufficient to ensure that he can properly carry out his functions. Those functions include those set out in s. 57(2), which provides in relevant part:

> "*…the [Commissioner] shall keep under review-*
>
> *(a) the exercise and performance by the Secretary of State of the powers and duties conferred or imposed on him by or under sections 1 to 11;*
>
> *…*
>
> *(d) the adequacy of the arrangements by virtue of which-*
>
> *(i) the duty which is imposed on the Secretary of State…by section 15[99]…*
>
> *[is] sought to be discharged*."

2.109 A duty is imposed on, among other persons, every person holding office under the Crown to disclose and provide to the Commissioner all such documents and information as he may require for the purpose of enabling him to carry out his functions: s. 58(1).

2.110 In practice, the Commissioner (via an inspection team of 2-3 people) has visited each Intelligence Service and the main Departments of State twice a year, for 3 days on each occasion (2014 Annual Report, §6.51 [***See Annex 12***]). Inspections are thorough and detailed. A typical inspection of an interception agency will include the following (see 2014 Annual Report, §6.46):

[99] This is a reference to both the s. 15 and the s. 16 arrangements, as the latter are required by s. 15(1)(b).

"- a review of the action points or recommendations from the previous inspection and their implementation;

- *an evaluation of the systems in place for the interception of communications to ensure they are sufficient for the purposes of RIPA and that all relevant records have been kept;*
- *examination of selected interception applications to assess whether they were necessary in the first instance and then whether the requests met the necessity and proportionality requirements;*
- *interviews with case officers, analysts and/or linguists from selected operations to assess whether the interception and justifications for acquiring all the material were proportionate;*
- *examination of any urgent oral approvals to check the process was justified and used appropriately;*
- *A review of those cases where communications subject to legal privilege or otherwise confidential information (e.g. confidential journalistic, or confidential medical) have been intercepted and retained, and any cases where a lawyer is the subject of an investigation;*
- *An investigation of the procedures in place for the retention, storage and destruction of intercepted material and related communications data;*
- *A review of the errors reported, including checking that the measures put in place to prevent recurrence are sufficient."*

2.111 Representative samples of warrantry paperwork are scrutinised (2014 Annual Report §6.52) including the paperwork for s. 8(4) warrants (Farr §91). The total number of warrants specifically examined equated in 2014 to 58% of the extant warrants at the end of the year, and 34% of new warrants issued in 2014 (2014 Annual Report, §6.53). The examination process is a 3-stage one, as the 2014 Report explains at §6.52:

" - First, to achieve a representative sample of warrants we select from across different crime types and national security threats. In addition we focus on those of particular interest or sensitivity, for example those which give rise to an unusual degree of collateral intrusion, those which have been extant for a considerable period (in order to assess the continued necessity for interception), those which were approved orally, those which resulted in the interception of legal or otherwise confidential communications, and so-called "thematic" warrants…

- *Second, we scrutinise the selected warrants and associated documentation in detail during reading days which precede the inspections.*
- *Third, we identify those warrants, operations or areas of the process where we require further information or clarification and arrange to interview relevant operational, legal or technical staff, and where necessary we require and examine further documentation or systems in relation to those matters during the inspections."*

2.112 The Commissioner also produces detailed written reports and recommendations after his inspections of the Intelligence Services, which are sent to the head of the relevant Intelligence Service and copied to the relevant Secretary of State and warrant granting department (2014 Annual Report at §6.47). The Commissioner meets with the relevant Secretaries of State (2014 Annual Report at §3.33).

2.113 In addition to these regular inspections, the Commissioner has power to (and does) investigate specific issues. Thus, the Commissioner has undertaken "extensive investigations" into the media stories derived from material said to have been disclosed by Edward Snowden, insofar as they concern allegations of interception by UK agencies. The conclusions of those investigations are set out in the Commissioner's 2013 Annual Report, especially Section 6 (***See Annex 11***).

2.114 S. 58 RIPA imposes important reporting duties on the Commissioner. (It is an indication of the importance attached to this aspect of the Commissioner's functions that reports are made to the Prime Minister.)

2.115 The Commissioner is by s. 58(4) under a duty to make a report every six months[100] to the Prime Minister regarding the carrying out of his functions. Pursuant to s. 58(6), a copy of each six-monthly report (redacted, where necessary, under s. 58(7)) must be laid before each House of Parliament. In this way, the Commissioner's oversight functions help to facilitate Parliamentary oversight of the activities of the Intelligence Services (including by the ISC). The Commissioner's practice is to make six-monthly reports in open form, with a closed confidential annex for the benefit of the Prime Minister going into detail on any matters which cannot be discussed openly.

[100] s.58 RIPA was amended with effect from 17 July 2014 to provide for six-monthly reports: previously, reports were annual.

2.116 Further, s. 58 provides:

> *"(2) If it at any time appears to the [Commissioner]-*
>
> *(a) that there has been a contravention of the provisions of this Act in relation to any matter with which the Commissioner is concerned, and*
>
> *(b) that the contravention has not been the subject of a report made to the Prime Minister by the Tribunal,*
>
> *he shall make a report to the Prime Minister with respect to that contravention.*
>
> *(3) If it at any time appears to the [Commissioner] that any arrangements by reference to which the duties imposed by [section 15]…have sought to be discharged have proved inadequate in relation to any matter with which the Commissioner is concerned, he shall make a report to the Prime Minister with respect to those arrangements."*

S. 58(5) grants the Commissioner power to make, at any time, any such other report to the Prime Minister on any other matter relating to the carrying out of his functions as he thinks fit.

2.117 In addition, the Commissioner is required by s. 57(3) to give the IPT:

> *"…such assistance (including his opinion as to any issue falling to be determined by the Tribunal) as the Tribunal may require-*
>
> *(a) in connection with the investigation of any matter by the Tribunal; or*
>
> *(b) otherwise for the purposes of the Tribunal's consideration or determination of any matter."*

2.118 The IPT is also under a duty to ensure that the Commissioner is apprised of any relevant claims / complaints that come before it: s. 68(3).

2.119 The Commissioner's oversight functions are supported by the record keeping obligations that are imposed as part of the s. 8(4) regime. See §2.85, §2.80 and §2.97 above; and §§6.27-6.28 of the Code. His oversight functions are further supported by the obligation to report any breaches of the ss. 15 and 16 arrangements pursuant to

§7.1 of the Code (see §2.80 above). In practice, all the agencies that are empowered to conduct interception have arrangements in place with the Commissioner to report errors that arise in their interception operations. The Commissioner addresses such errors in his six-monthly reports (see *e.g.* §§3.58-3.68 of the 2013 Annual Report [See Annex 11]).

The IPT and interception under s. 8(4) warrants

2.120 As regards the s. 8(4) regime, the following specific aspects of the IPT's jurisdiction are of particular relevance. The IPT has exclusive jurisdiction to consider claims under s. 7(1)(a) HRA that relate to conduct for or in connection with the interception of communications in the course of their transmission by means of a telecommunication system:

(1) which has taken place with the authority, or purported authority of an interception warrant (ss. 65(2)(b), 65(3)(d), 65(5)(b), 65(7)(a) and 65(8)(a) RIPA); or
(2) which has taken place in circumstances where it would not have been appropriate for the conduct to take place without an interception warrant or without proper consideration having been given to whether such authority should be sought (ss. 65(2)(a), 65(3)(d), 65(5)(b), 65(7)(b) and 65(8)(a) RIPA).

2.121 The IPT may consider and determine any complaints by a person who is aggrieved by any conduct for or in connection with the interception of communications in the course of their transmission by a telecommunication system which he believes to have taken place in relation to him, to any of his property, to any communications sent by or to him, or intended for him, or to his use of any telecommunications service or system and to have taken place:

(1) with the authority, or purported authority of an interception warrant (ss. 65(2)(b), 65(4), 65(5)(b), 65(7)(a) and 65(8)(a) of RIPA); or
(2) in circumstances where it would not have been appropriate for the conduct to take place without an interception warrant or without proper consideration having been given to whether such authority should be sought: ss. 65(2)(b),

65(4), 65(5)(b), 65(7)(b) and 65(8)(a) of RIPA).

2.122 The IPT may thus entertain any ECHR claim or public law complaint about the operation or alleged operation of the s. 8(4) regime. This may include investigating whether the Intelligence Services have complied with the ss. 15 and 16 safeguards in any particular case.

2.123 Under s. 67(7) RIPA, the IPT may (in addition to awarding compensation or making any other order that it thinks fit) make an order quashing or cancelling any warrant and an order requiring the destruction of any records of information which has been obtained in exercise of any power conferred by a warrant.

2.124 Further, where a claimant / complainant succeeds before the IPT and the IPT's determination relates to any act or omission by or on behalf of the Secretary of State, or to conduct for which any warrant was issued by the Secretary of State, the IPT is by s. 68(5) RIPA required to make a report of their findings to the Prime Minister.

3 PART 3 – RESPONSE TO THE GROUNDS

QUESTION 1. THE INTELLIGENCE SHARING REGIME

The Applicants do not have victim status

3.1 The Applicants do not contend, and have put forward no evidential basis for contending, that their communications have in fact been intercepted under the Prism or Upstream programmes, and subsequently shared with the Intelligence Services. Rather, they assert only that they "believe" that this is the case, but no evidential basis is provided for that assertion: see Additional Submissions on the Facts and Complaints at §7. In the circumstances, that mere assertion does not begin to establish that the Applicants are "directly affected" by the Intelligence Sharing Regime, such that they have victim status for the purposes of Article 34 ECHR.

3.2 The Grand Chamber has recently clarified the conditions under which an applicant can claim to be a victim of secret surveillance measures violating Article 8 ECHR, without having to prove that secret surveillance measures have in fact been applied to him: see *Zakharov v Russia* (app. 47143/06, 4 December 2015). *Zakharov* notes, and resolves, a potential divergence in the Court's case law between those cases suggesting that general challenges to the relevant legislative regime would be permitted in such circumstances, and those suggesting that the relevant security agencies must be reasonably likely to have applied the measures in question to the applicant: see *Zakharov* at §§164-172.

3.3 Two conditions must be satisfied before an applicant can claim to be the victim of a relevant violation without needing to show his communications have been interfered with – see *Zakharov* at §171:

> *"Accordingly, the Court accepts that an applicant can claim to be the victim of a violation occasioned by the mere existence of secret surveillance measures, or legislation permitting secret surveillance measures, if the following conditions are satisfied. Firstly, the Court will take into account the scope of the legislation permitting secret surveillance measures by examining whether the applicant can possibly be affected by it, either because he or she belongs to a group of persons targeted by the contested legislation or because the legislation directly affects all users of communication services by instituting a system where any person can have his or her communications intercepted. Secondly, the Court will take into account the availability of remedies at the national level and will adjust the degree of scrutiny depending on the effectiveness of such remedies."*

3.4 As to the second condition, where the domestic system affords no effective remedy to a person who suspects he has been the victim of secret surveillance, an exception to the rule that individuals may not challenge a law *in abstracto* is justified. However, if the national system provides for effective avenues for challenge and remedies, as in the present case, an individual may claim to be a victim of a violation occasioned by the mere existence of secret measures only if he is able to show that, due to his personal situation, he is potentially at risk of being subjected to such measures: *Zakharov* at §171.

3.5 Here, neither of the two conditions in §171 of *Zakharov* is satisfied. **First**, the Applicants do not belong to the group of persons who may be said to be possibly affected by the Intelligence Sharing Regime. They have put forward no basis on which they are at realistic risk of having their communications intercepted under the Prism or Upstream programmes, and shared with the Intelligence Services. In particular:

(1) The Prism and Upstream programmes permit the interception and acquisition of communications to, from or about specific tasked selectors associated with non-US persons who are reasonably believed to be outside the US - i.e. they concern unanalysed intercepted communications (and associated communications data) relating to particular individuals outside the US, not broad data mining.

(2) As stated in the Disclosure, the Intelligence Services have only ever made a request for such unanalysed intercepted communications (and associated communications data) where a RIPA warrant is already in place for that material, but the material cannot be collected under the warrant[101]. Any request made in the absence of a warrant would be exceptional, and would be decided upon by the Secretary of State personally: see the Code at §12.3.

(3) The conditions for intercepting communications pursuant to a RIPA warrant are as set out in s.5(3) RIPA. They are the interests of national security; the prevention or detection of serious crime; or the safeguarding of the UK's economic well-being, in circumstances appearing relevant to the interests of national security. Further, as set out below at §§4.17-4.19, those conditions substantially mirror, and are no narrower than, the statutory functions of the Intelligence Services under the SSA and ISA.

(4) None of the Applicants suggest that their data could be collected and shared under any of the conditions in s.5(3) RIPA, the SSA or ISA. They suggest that their data may be shared with the UK because of their human rights activities. But such activities would not give any grounds for the issue of a warrant for interception of the Applicants' communications under s.5(3) RIPA. Nor, by the same token, would they give grounds for intelligence

[101] See the IPT's 5 December Judgment, §48(2).

sharing without a warrant in pursuance of the Intelligence Services' statutory functions. The Applicants do not contend otherwise.

3.6 **Secondly**, the Applicants did complain at the national level about whether they might have been subject to unlawful intelligence sharing, but no such determination was made by the IPT. Had there been unlawful sharing of their data, the IPT would have so declared, and would been empowered to make any order it saw fit, including an order for compensation, and the destruction of the data in question (see s.67(7) RIPA). Thus, for example, the IPT would have declared the sharing of the Applicants' data with the Intelligence Services to be unlawful in any of the following circumstances:

(1) Data was shared where a warrant covering the Applicant's communications was in place, but the conditions for the issue of a warrant were not met.
(2) Data was shared where a warrant covering the Applicant's communications was in place, and the conditions for the issue of a warrant were met, but the particular data could not lawfully and proportionately be shared pursuant to the relevant Intelligence Service's statutory functions.
(3) Data was shared where no warrant covering the Applicant's communications was in place, and the Secretary of State had not personally decided that a request for the Applicant's communications should be made.
(4) Data was shared where no warrant covering the Applicant's communications was in place, the Secretary of State had personally decided that a request for the Applicant's communications should be made, but such a request was not lawful and proportionate in pursuance of the Intelligence Services' statutory functions.

3.7 The effectiveness of the IPT in investigating allegations of unlawful intelligence sharing in these circumstances is amply demonstrated by its careful and exhaustive consideration of the relevant legal regime and the treatment of the applicants' own communications in the Liberty proceedings. The fact that the IPT is (and has shown itself to be) an effective domestic route of challenge makes it unnecessary and inappropriate for the Court to entertain an abstract challenge to the Intelligence

Sharing Regime as a whole, brought by Applicants who have failed to put forward a plausible case that their data has been shared pursuant to that regime.

The "in accordance with the law" and "necessity" tests

The Intelligence Sharing Regime is "in accordance with the law"

3.8 The expression "in accordance with the law" requires:

> *"…firstly, that the impugned measure should have some basis in domestic law; it also refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must, moreover, be able to foresee its consequences for him, and compatible with the rule of law…"* (*Weber*, §84).

3.9 The interferences plainly have a *basis in domestic law*. The statutory provisions in the Intelligence Sharing Regime provide domestic law powers for the obtaining and subsequent use of communications and communications data in issue (assuming that this is necessary for one or more of the functions of the Intelligence Service in question, and proportionate for the purposes of inter alia s.6(1) HRA).

3.10 The law in question is clearly "*accessible*". It is set down in statute, and supplemented by chapter 12 of the Code. (Indeed, even prior to the issue of chapter 12 of the Code, it was "accessible" as a result of the Disclosure[102], contrary to the submissions made at §72(3) of the Applicants' Additional Submissions. For these purposes, case law may form part of a corpus of accessible law: see e.g. *Huvig v France* 24 April 1990, Series A no. 176-B at §28, *Uzun v Germany* app. 35623/05, ECHR 2010, at §33.)

3.11 As to *"foreseeability"* in this context, the essential test, as recognised in §68 of *Malone v UK* (app. 8691/79), is whether the law indicates the scope of any discretion and the manner of its exercise with sufficient clarity "*to give the individual adequate protection against arbitrary interference*". The Grand Chamber has confirmed in *Zakharov* that this test remains the guiding principle when determining the foreseeability of

[102] Further, the Disclosure was embodied in a draft of the Code, published in February 2015, with which the Government undertook to comply.

intelligence-gathering powers (see §230). Further, this essential test must always be read subject to the important and well-established principle that the foreseeability requirement cannot mean that an individual should be enabled to foresee when the authorities are likely to resort to secret measures so that he can adapt his conduct accordingly: *Malone* at §67; *Leander v. Sweden*, 26 March 1987, Series A no.116, at §51; and *Weber* at §93. The Intelligence Sharing Regime satisfies this test.

3.12 **First**, the regime is sufficiently clear as regards the circumstances in which the Intelligence Services can in principle **obtain** information from the US authorities, which has been gathered under the Prism or Upstream programmes.

3.13 The purposes for which such information can be obtained are explicitly set out in ss.1-2 SSA, and ss.1-2 and 3-4 ISA (see above), which set out the functions of the Intelligence Services. They are the interests of national security, in the context of the various Intelligence Services' particular functions; the interests of the economic wellbeing of the United Kingdom; and the prevention and detection of serious crime. Thus, it is clear that e.g. GCHQ may in principle - as part of its function (in s. 3(1)(a) of ISA) of obtaining information derived from communications systems[103] - obtain communications and communications data from a foreign intelligence agency if that is "*in the interests of national security*", with particular reference to the Government's defence and foreign policies (s.3(2)(a) ISA), or "*in the interests of the economic well-being of the United Kingdom*" (s.3(2)(b) ISA), or "*in support of the prevention or detection of serious crime*" (s. 3(2)(c) of ISA); provided always that it is also necessary and proportionate to obtain information for that purpose under s. 6(1) of the HRA. It will be noted that these purposes are no wider in substance than the statutory purposes for which an interception warrant could be issued under s.5 RIPA (prior to its amendment by DRIPA – see §2.53 above). Indeed, in certain respects, they are more tightly defined than the conditions for obtaining a warrant under s.5 RIPA (see *e.g.* s. 1(2) of the SSA, and 1(2)(a) and 3(2)(a) of the ISA, as compared with s. 5(3)(a) of RIPA[104]).

[103] Such systems fall within the scope of the s. 3(1)(a) of ISA by virtue of being "equipment" producing "electromagnetic, acoustic and other emissions".

[104] By s. 1(2) of the SSA, one of the Security Service's functions is "the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine

3.14 The statutory purposes for issue of a warrant under s.5 RIPA (in its unamended form) were considered by the Court in *Kennedy* and were found to be sufficiently detailed to satisfy the requirement of foreseeability, even in the context of interception of communications by the defendant state itself - see *Kennedy* at §159:

> *"As to the nature of the offences, the Court emphasises that the condition of foreseeability does not require states to set out exhaustively by name the specific offences which may give rise to interception. However, sufficient detail should be provided of the nature of the offences in question. In the case of RIPA, s.5 provides that interception can only take place where the Secretary of State believes that it is necessary in the interests of national security, for the purposes of preventing or detecting serious crime or for the purposes of safeguarding the economic well-being of the United Kingdom. The applicant criticises the terms "national security" and "serious crime" as being insufficiently clear. The Court disagrees…"*

3.15 The Court has more recently found those very same purposes sufficiently detailed to satisfy the "foreseeability" test in the context of covert surveillance pursuant to Part II RIPA: see *RE v United Kingdom* app. 62498/11, 27 October 2015, at §133 (citing *Kennedy* with approval). See too e.g. *Esbester v UK* (app. 18601/91), April 1993, where the Commission found the statutory functions of the Security Service under the SSA to satisfy the demands of foreseeability in the context of security checking. (By contrast, the cases upon which the Applicants rely at §126 of their Application – *Khan v United Kingdom* (app. 35304/97), ECHR 2000-V and *Halford v United Kingdom,* 25 June 1997, Reports of Judgments and Decisions 1997-III – are both ones concerning police surveillance, where there was at the relevant time no statutory framework regulating the conduct in question.)

3.16 Moreover, the circumstances in which the Intelligence Services may obtain information under the Intelligence Sharing Regime are further defined and

---

parliamentary democracy by political, industrial or violent means" (emphasis added). Similarly, the statutory definition of the national security functions of SIS and GCHQ refer to "the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom" (emphasis added). Compare s. 5(3)(a) of RIPA, which identifies "the interests of national security" as a ground for interception, without further elaboration.

circumscribed by the Code and Disclosure (which reflect what has always been the practice of the Intelligence Services). In particular, the Code provides the following public safeguards on obtaining information:

(1) Save in exceptional circumstances, the Intelligence Services will only make a request for unanalysed intercepted communications and associated communications data, otherwise than in accordance with an international mutual legal assistance agreement, if a RIPA warrant is already in place covering the target's communications; the assistance of the foreign intelligence agency is necessary to obtain the communications because they cannot be obtained under that RIPA warrant; and it is necessary and proportionate for the Intelligence Services to obtain those communications. It should be noted that the circumstances are sufficiently exceptional that they have not yet ever occurred[105].

(2) If the Intelligence Services were to make a request for such material in the absence of a RIPA warrant, they would only do so if the request did not amount to a deliberate circumvention of RIPA or otherwise frustrate the objectives of RIPA (see §2.21 above). So, for example, the Intelligence Services could not make a request for material equally available by interception pursuant to a RIPA warrant. However, they could make a request for material which it was not technically feasible to obtain under Part I RIPA, and which it was necessary and proportionate for them to obtain pursuant to s.6 HRA.

(3) Further, if the Intelligence Services were to make a request for such material in the absence of a RIPA warrant, that request would be decided upon by the Secretary of State personally; and if the request was for "untargeted" material, any communications obtained would not be examined according to any factors mentioned in s.16(2)(a) and (b) RIPA, unless the Secretary of State personally considered and approved the examination of those communications by reference to such factors. In short, the same safeguards would be applied by analogy, as if the material had been obtained pursuant to a RIPA warrant.

[105] See §48(2) of the IPT's 5 December judgment.

3.17 **Secondly**, the Intelligence Sharing Regime is similarly sufficiently clear as regards the subsequent handling, use and possible onward disclosure of communications and communications data obtained by the Intelligence Services.

3.18 Handling and use is addressed by (i) s. 19(2) of the CTA, as read with the statutory definitions of the Intelligence Services' functions (in s. 1 of the SSA and ss. 1 and 3 of ISA); (ii) the general proportionality constraints imposed by s. 6 of the HRA and - as regards retention periods in particular - the fifth data protection principle; and (iii) the seventh data protection principle (as reinforced by the criminal offence in ss. 1(1) and 8(1) of the OSA) as regards security measures whilst the information is being stored.

3.19 Thus, for instance, it is clear that information (including communications / communications data) obtained by *e.g.* SIS from a foreign intelligence agency, for national security purposes (within the meaning of s. 1(2)(a) of ISA), relating to the actions of persons outside the British Islands (within the meaning of s. 1(1)(a) of ISA) may be used by SIS in support of the prevention of serious crime that may be committed by persons outside the British Islands (s. 19(2) of the CTA as read with s. 1(1)(a) and s. 1(2)(c) of ISA), insofar as such use would be proportionate under s. 6(1) of the HRA. Indeed, when analysed in this way, it is difficult to see what public interest would be served by further constraining the powers of the Intelligence Services to use information. In particular, to return to the example just provided, it is difficult to see why SIS should not in principle be permitted to use the information in question in all cases in which such use would be proportionate in order to support the prevention or detection of serious crime within the scope of SIS's functions (as set out in s. 1(1) of the ISA). Similarly, it is clear that information that has been obtained by *e.g.* SIS from a foreign intelligence agency, and that is being retained by SIS for its functions (as defined in s. 1(1) of the ISA) insofar as they are exercised for the purpose of national security (within the meaning of s. 1(2)(a) of ISA), cannot be retained for longer than is necessary for that purpose, given the fifth data protection principle.

3.20 Further, ss. 1-2 of the SSA and ss. 1-2 and 3-4 of the ISA, as read with ss. 19(3)-(5) of the CTA and s. 6(1) of the HRA, sufficiently address the circumstances in which the

Intelligence Services may disclose information obtained from a foreign intelligence agency to others. In addition, disclosure in breach of the "arrangements" for which provision is made in s. 2(2)(a) of the SSA and ss. 2(2)(a) and 4(2)(a) of the ISA is rendered criminal by s. 1(1) of the OSA. Thus, for instance, it is clear that information obtained by *e.g.* SIS from a foreign intelligence agency, for national security purposes (within the meaning of s. 1(2)(a) of ISA), relating to the actions of a person outside the British Islands (within the meaning of s. 1(1)(a) of ISA) may be disclosed by SIS to another body for the purpose of the prevention of serious crime (s. 2(2)(a)(iii) of ISA and s. 19(4)(c)), insofar as such disclosure would be proportionate under s. 6(1) of the HRA.

3.21 Moreover, additional safeguards as to the handling, use and onward disclosure of material obtained under the Intelligence Sharing Regime are provided by the Code. Specifically, chapter 12 of the Code provides that where the Intelligence Services receive intercepted communications content or data from a foreign state, irrespective whether it is solicited or unsolicited, analysed or unanalysed, and whether or not the communications data is associated with the content of communications, the communications content and data are subject to exactly the same internal rules and safeguards as the same categories of content or data, when the material is obtained directly by the Intelligence Services as a result of interception under RIPA. That has important consequences:

(1) It means that the safeguards set out in s.15 RIPA, as expanded upon in Chapter 7 of the Code, apply to intercept material obtained under the Intelligence Sharing Regime. So for example, just as under RIPA:

i. The number of persons to whom the material is disclosed or otherwise made available, the extent to which it is made available, the extent to which it is copied, and the number of copies that are made, must be limited to the minimum necessary for the purposes authorised in s.15(4) RIPA.

ii. The material (and any copy) must be destroyed as soon as there are no longer any grounds for retaining it as necessary for any of the authorised purposes in s.15(4) RIPA.

iii. The arrangements for ensuring that (i) and (ii) above are satisfied

must include such arrangements as the Secretary of State considers necessary to ensure the security of retained material: see s.15(5) RIPA.

iv. The disclosure of intercepted material to authorities outside the UK is subject to the safeguards set out in §7.5 of the Code.

(2) It means that the internal rules and safeguards applicable to material obtained under the Intelligence Sharing Regime are *de facto* subject to oversight by the Commissioner, who offers an "*important safeguard against abuse of power*": see s.57(2)(d) RIPA and *Liberty v UK* app. 58243/00, 1 July 2008 at §67.

3.22 **Thirdly**, when considering whether the Intelligence Sharing Regime is "*foreseeable*", the Court should take into account the available oversight mechanisms – namely, the ISC, the IPT, and (as set out above, with respect to oversight of the relevant internal "arrangements" themselves) the Commissioner. The relevance of oversight mechanisms in the assessment of foreseeability, and in particular the existence of adequate safeguards against abuse, is well established in the Court's case law: see e.g. *Kennedy*: when considering the general ECHR-compatibility of the RIPA s. 8(1) regime, the Court at §§155-170 of *Kennedy* "*jointly*" considered the "*in accordance with the law*" and "*necessity*" requirements, and in particular analysed the available oversight mechanisms (at §§165-168) in tandem with considering the foreseeability of various elements of the regime (§§156-164). See too the Grand Chamber's judgment in *Zakharov*, where the Court examined "*with particular attention*" the supervision arrangements provided by Russian law, as part of its assessment of the existence of adequate safeguards against abuse: §§271-280.

3.23 The statutory oversight mechanisms of the ISC and IPT are important and effective, and the Applicants' criticisms of them in their Application and Update Submissions are misplaced.

3.24 As concerns the *ISC*:

(1) The ISC sets its own agenda and work programme and provides an effective strand of the relevant oversight (see Farr §70 and Domestic Law and Practice above).

(2) Indeed, it proactively determined to address allegations both about the alleged Tempora operation and about intelligence sharing in the context of Prism, and has done so in very considerable detail, with the benefit of evidence from many interested parties in its Statement of 17 July 2013 and the ISC Report. The Report addresses the activities of all the Intelligence Services; and was written with the benefit of 56 substantive submissions from parties including privacy advocates, NGOs and the media, and after a number of public evidence sessions, taking evidence from "*both sides of the debate*": see ISC Report, §14[106].

(3) It may be noted that in the Statement of 17 July 2013 the ISC expressed itself satisfied that it had received full information about "*the whole range of Agency capabilities, how they are used and how they are authorised*": see ISC Report, §12. That reflects the obligation on the Heads of the Intelligence Services to arrange for any information requested by the ISC in the exercise of its functions to be made available to it (see Mr Farr, *§67*).

3.25 The *IPT* has broad jurisdiction and extensive powers (including to require the Intelligence Services to provide it with all relevant information to determine complaints). Any person may bring a claim in the IPT: and they need not be able to adduce any evidence that the Intelligence Services have engaged in relevant "conduct" in relation to them, in order to have their complaint considered and determined. The governing provisions have been dealt with above. Its rigorous and detailed judgments in the domestic proceedings plainly indicates that it provides an effective safeguard against abuse.

3.26 The *Commissioner* also offers an effective mechanism for overseeing the internal arrangements under s.15 RIPA. The fact that those same arrangements are *de facto* subject to oversight by the Commissioner in the context of material obtained under the Intelligence Sharing Regime is yet another safeguard against abuse.

3.27 The Court should also take into account in the foreseeability test, just as it did in *Kennedy* at §168, the fact that the investigations by the oversight bodies have not revealed any deliberate abuse by the Intelligence Services of their powers. Neither

[106] ***[See Annex 13]***

the ISC nor Commissioner has found that the Intelligence Services have circumvented or attempted to circumvent UK law by receiving material under the Intelligence Sharing Regime, despite the fact that both of them have investigated this allegation - see in particular:

(1) the ISC's finding in its Statement of 17 July 2013 that the UK "*has not circumvented or attempted to circumvent UK Law*" by receiving material from the US[107];

(2) The Commissioner's rejection of the allegation that the Intelligence Services "*receive from US agencies intercept material about British citizens which could not lawfully be acquired by intercept in the UK ... and thereby circumvent domestic oversight regimes*" (see his 2013 Annual Report at §§6.8.1-6.8.6[108]).

3.28 **Finally**, for the purposes of the foreseeability test, the Court should take into account too that the IPT has examined the Intelligence Services' internal safeguards in the context of the Intelligence Sharing Regime in detail, and has found that adequate internal safeguards exist[109], and that the Regime as a whole (with the benefit of the Disclosure, now mirrored in the Code) is in accordance with the law. The fact that the applicable internal safeguards have now been examined not just by the Commissioner, but also by the domestic courts, and have been found to offer sufficient protection for the purposes of rights under the ECHR, is an important indicator that the regime as a whole provides adequate safeguards against abuse.

Specific points made in the Applicants' Additional Submissions on the Facts and Complaints

3.29 The Applicants assert that the IPT's approach to the intelligence sharing regime was based on a "fundamental error" because they say that the IPT wrongly applied a "significantly attenuated" version of the *Weber* criteria (i.e. the six "minimum

[107] See ***[Annex 21]***. The investigation that preceded the ISC's Statement was thorough. See §5 of the Statement.

[108] [***See Annex 11]***

[109] See §55 of the IPT's 5 December Judgment:
"Having considered the arrangements below the waterline, as described in the judgment, we are satisfied that there are adequate arrangements in place for the purpose of ensuring compliance with the statutory framework and with Articles 8 and 10 of the Convention, so far as the receipt of intercept from Prism and/or Upstream is concerned."

safeguards" to which the Court referred at §95 of *Weber*[110]) (see §71 of the Applicants' Additional Submissions). That argument is unsustainable. The IPT was entirely correct to conclude at §41 of the 5 December Judgment that in this context the *Weber* criteria (or "*nearly Weber*" criteria) do not apply. And even if such criteria were to apply, it would not be necessary or appropriate to set them out in statute.

3.30 *Weber* concerns interception **by the respondent State**. The Applicants do not cite any Art. 8 case that concerns a complaint that the intelligence agencies of the respondent State had obtained information from **another** State (whether in the form of communications that that other State had itself intercepted, or otherwise). Indeed, so far as the Government are aware, the application of Art. 8 to cases of this latter type has never been considered by the Court.

3.31 It is submitted that, not merely is there no authority indicating that the specific principles that have been developed in cases involving interception by the respondent State are to be applied in the distinct factual context where the intelligence agencies of the respondent State have merely obtained information from a foreign State, but there are also very good reasons why that should not be so.

3.32 **First**, the Court has expressly recognised that the "rather strict standards" developed in the recent Strasbourg intercept cases do not necessarily apply in other intelligence-gathering contexts: *Uzun v. Germany* at §66. The Court has never suggested that this form of wide-ranging and detailed statutory scheme is necessary for intelligence sharing with foreign intelligence agencies (and see §96 of *S and Marper v. UK* (GC) nos. 30562/04 and 30566/04, ECHR 2008: domestic legislation "*cannot in any case provide for every eventuality*").

3.33 **Secondly,** the Court has made clear subsequent to *Weber* in *Liberty, Kennedy* and *Zakharov* that even in the context of interception by the respondent State it is not

[110] "*the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed …*" (*Weber*, at §95).

necessary for every provision/rule to be set out in primary legislation. The test is whether there is a sufficient indication of the safeguards *"in a form accessible to the public"*: see *Liberty* at §§67-69; see also §157 of *Kennedy* as regards the Code. That position has now been confirmed by the Grand Chamber in *Zakharov,* which refers to the need for the *Weber* criteria to be set out *"in law"*, rather than in statute: see *Zakharov* at §231.

3.34 **Thirdly**, there is no good reason to single out intercepted communications / communications data from other types of information that might in principle be obtained from a foreign intelligence agency, such as non-intercept communications/communications data, intelligence from covert human intelligence sources (as they would be termed under RIPA) or covert audio / visual surveillance. In many contexts, the Intelligence Services may not even know whether communications or communications data provided to them by a foreign intelligence agency have been obtained as a result of interception. Moreover, as Mr Farr explains, neither the sensitivity of the information in question, nor the ability of a person to predict the possibility of an investigative measure being directed against him, distinguish communications and communications data from other types of intelligence (Mr Farr §§27-30). Thus, it would be nonsensical if Member States were required to comply with the *Weber* criteria for receipt of intercept material from foreign States; but were not required to do so for any other type of intelligence that foreign States might share with them.

3.35 If the *Weber* criteria apply to the obtaining of intercept material from a foreign intelligence agency, and if the Intelligence Sharing Regime does not satisfy those criteria, then it is difficult to see how the Intelligence Services could lawfully obtain <u>any</u> information from a foreign intelligence agency about an individual that derived from covert human intelligence sources, covert audio / visual surveillance or covert property searches. But that would be a remarkable, and deeply concerning, conclusion - not least given that intelligence sharing is (and has for many years been) vital to the effective operation of the Intelligence Services (see Mr Farr *§§15-26*).

3.36 **Fourthly**, it would plainly not be feasible (or, from a national security perspective, safe) for a domestic legal regime to (i) set out in publicly accessible form (let alone set

out in statute) all the various types of information that might be obtained, whether pursuant to a request or not, from each of the various foreign States with which the State at issue might share intelligence, (ii) define the tests to be applied when determining whether to obtain each such type of information and the limits on access and (iii) set out the handling, etc. requirements and the uses to which all such types of information may be put: see the reasons already set out at §4.102 above, and expanded upon by Mr Farr at §§56-61.

3.37 **Finally,** if (contrary to the above) the *Weber* criteria were to apply in this context, the Intelligence Sharing Regime satisfies each of the six criteria through a combination of the statutory provisions governing the receipt of intelligence, and the Code, for the reasons already set out at §§3.8-3.28 above. It describes:

(1) the nature of the offences which may lead to intelligence being obtained and the persons whose communications may be obtained. Those matters are implicit within the statutory description of the purposes of which intelligence may be obtained: see §§3.12-3.16 above;
(2) the limits on the duration of such obtaining (since a RIPA warrant will be in place, save in exceptional circumstances, and such a warrant has clear limits on duration);
(3) the process for examining, using and storing data (since parallel safeguards to those under RIPA apply); and
(4) the circumstances in which the material may be erased/destroyed (since the material is treated in the same way as comparable material obtained under RIPA).

3.38 In terms of the Applicants' reasons for suggesting that the Intelligence Sharing Regime is "not in accordance with the law" (see §72 of the Applicants' Additional Submissions), the Government repeats §§3.8-3.28 above. The Code itself is "law" for the purposes of the "in accordance with the law" test: see e.g. *Kennedy*. So, to the extent that the Intelligence Services' internal arrangements are set out in the Code, they are indeed "law". Moreover, the Disclosure is also "law" for these purposes: it is a published statement, contained in publicly accessible court judgments: see §3.10 above.

3.39 There is a very good reason why the Code summarises certain important aspects of the internal arrangements, rather than setting them out in full. To set them out in full would have the effects set out by Mr Farr at §§55-61, and correspondingly undermine the interests of national security. It would reveal existing intelligence relationships; show hostile individuals what sort of information is shared, and how; damage relations with intelligence partners; reduce the quality of and quantity of intelligence available to the Intelligence Services; limit operational flexibility; and risk offering additional insights into the activities of the Intelligence Services whenever they were revised. Further, the IPT agrees. It investigated the internal arrangements, and found that further disclosure would risk damaging national security and the NCND principle (see the 5 December Judgment, §50(iv)).

3.40 Moreover, even if unpublished arrangements are not themselves "law", they are plainly relevant both to the foreseeability of the Intelligence Sharing Regime and the fulfilment of the underlying purpose for which the "in accordance with law" requirement exists in this context, namely to protect against arbitrary or abusive conduct by the State. The fact that further internal arrangements are known to exist, have been assessed by the IPT, and are subject to oversight as set out above is itself a relevant safeguard against abuse: see above.

The "necessity" test

3.41 The Applicants rightly make no submissions on the "necessity" of the Intelligence Sharing Regime. No separate question of "necessity" arises with regard to the Intelligence Sharing Regime, distinct from the issue whether the regime is "in accordance with the law". If the regime itself is "in accordance with the law" (as it is), any issue of necessity would arise only on the individual facts concerning any occasion where intelligence was shared, since the sharing of intelligence may obviously be necessary and proportionate in some cases, but not others[111]. To that

[111] Note however Farr §§15-25 regarding the general importance to the UK's national security interests of the intelligence it receives from the US authorities, which he states has led directly to the prevention of terrorist attacks and the saving of lives.

end it is pertinent that the Applicants' individual allegations of unlawful intelligence sharing were not upheld in the domestic IPT proceedings.

4 QUESTION 2. THE SECTION 8(4) REGIME

Victim status

4.1 The conditions under which an applicant can claim to be a victim of secret surveillance measures violating Article 8 ECHR have been addressed in detail above at §§3.2-3.4 in the context of the Intelligence Sharing Regime, with particular reference to the Grand Chamber decision in *Zakharov*. In the context of the s.8(4) Regime and on the basis of the assumed facts at §§1.26-1.28 and §§2.77-2.78 above, the key stage is evidently the selection and examination stage i.e. the point at which a person actually reads, looks at, or listens to intercepted material. Therefore, in this context (and as with the Intelligence Sharing Regime), a person needs to be able to demonstrate that they are at realistic risk of selection/examination which means being able to demonstrate that they have reason to believe their communications are of interest to the Intelligence Services on the grounds mentioned in s.5(3)(a), (b) or (c) (i.e. in the interests of national security, for the purposes of preventing or detecting serious crime or for the purpose of safeguarding the economic well-being of the United Kingdom); grounds which mirror the statutory functions of the Intelligence Services. Unless those grounds are satisfied then any selection and examination would be unlawful. For the reasons set out at §3.5(4) above, none of the Applicants can satisfy that test (save in this s.8(4) context for the Legal Resources Centre and Amnesty International, given the IPT's conclusions in the 22 June 2015 judgment (see §1.50 above)).

The "in accordance with law" and "necessity" tests

4.2 Before addressing the application of the "in accordance with the law" and "necessity" tests under Article 8 ECHR in detail, five preliminary points should be noted at the outset:

i. Some form of s. 8(4) Regime is a practical necessity.

ii. The s. 8(4) Regime was designed on this basis, and with the internet in mind.

iii. The existing ECtHR interception case law - and in particular *Weber*, *Liberty* and *Kennedy* - supports the Government's position that the "*in accordance with the law*" requirement is satisfied.

iv. By contrast, *Digital Rights Ireland* is not relevant to this issue.

v. Intercepting communications (*i.e.* obtaining the content of communications) is in general more intrusive - and is thus deserving of greater protection - than obtaining communications data.

i. The practical necessity of some form of S. 8(4) Regime

4.3 The s.8(4) Regime in principle permits a substantial volume of communications to be intercepted, and then requires the application of a selection process to identify a smaller volume of intercepted material that can actually be examined by persons, with a prohibition on the remainder being so examined. To this extent, it differs from the regime that applies under s. 8(1) RIPA, under which interception warrants target a specified person or single set of premises.

4.4 The crucial point is that this difference does not reflect some policy choice on the UK Government's part to undertake a programme of "*mass surveillance*" in circumstances where a s. 8(1) warrant would be perfectly well suited to acquiring the external communications that are needed for the purposes of national security, etc.

4.5 The fact is that the Government has no choice in this regard if it is to obtain the external communications it considers necessary for safeguarding the UK's national security. The reasons why that is the case follow from the summary of the facts at §§1.29-1.35 above. As the Commissioner has confirmed, following an "*in detail*" investigation of the relevant (and sensitive) technical background relating to the procedure under the s. 8(4) Regime, *there are no other reasonable means that would enable the Intelligence Services to have access to external communications that it is adjudged necessary to secure*. That is because (in simplified summary) (i) communications are sent over the internet in small pieces (i.e. "packets"), which may be transmitted

separately, often by separate routes; (ii) in order to intercept a given communication of a target, while in transit over the internet, it is necessary to obtain all the "packets" associated with it, and reassemble them; and (iii) in order to reassemble the "packets", it is necessary to intercept the entirety of the contents of a bearer or bearers in order to discover whether any are intended for the target in question.

4.6 It is for these reasons that the Intelligence Services intercept the entirety of the contents of a bearer or bearers, and then subject them to an automated filtering process (resulting in much of the intercepted material being immediately discarded) in order to obtain any of the communications in which they are interested, while they transit the internet. The only practical way to find and reconstruct most external communication "needles" is to look through the communications "haystack".

4.7 So unless it is said that the Intelligence Services should not be able to obtain the external communications that they need to protect the UK's national security, the Applicants must accept *some* form of interception regime that permits substantially more communications to be intercepted (including, potentially, internal communications) than are actually being sought. Or, to continue the analogy in the paragraph above, they must accept a regime that permits the acquisition of "haystacks" in order to find communications "needles".

4.8 In addition, as Mr Farr explains and as the IPT accepted in the 5 December Judgment, there are important practical differences between the ability of the Intelligence Services to investigate individuals and organisations within the British Islands as compared with those abroad: see Mr Farr §§142-147. Those practical differences offer further justification for a regime of the form of the s. 8(4) Regime (Mr Farr §149): see §1.32 above.

ii. The s. 8(4) Regime was designed with the internet in mind, and on the basis that some form of s. 8(4) Regime was required

4.9 The s. 8(4) regime was - to Parliament's knowledge – designed to accommodate the internet, and Parliament was made aware of the issue just noted: see Lord Bassam in Lords Committee (Hansard, 12 July 2000 at column 323[112]):

> *"It is just not possible to ensure that only external communications are intercepted. That is because modern communications are often routed in ways that are not all intuitively obvious…. An internal communication--say, a message from London to Birmingham--may be handled on its journey by Internet service providers in, perhaps, two different countries outside the United Kingdom. We understand that. The communication might therefore be found on a link between those two foreign countries. Such a link should clearly be treated as external, yet it would contain at least this one internal communication. There is no way of filtering that out without intercepting the whole link, including the internal communication.*
>
> *Even after interception, it may not be practically possible to guarantee to filter out all internal messages. Messages may well be split into separate parts which are sent by different routes. Only some of these will contain the originator and the intended final recipient...."*

4.10 Unsurprisingly, given the above, the Commissioner concluded in his 2013 Annual Report that RIPA had not become "*unfit for purposes in the developing internet age*": see the Report at §6.5.55[113]. The fact that there the internet has grown in scale does not render the safeguards under RIPA less relevant or adequate.

iii. *Weber*, *Liberty* and *Kennedy* support the Government's position

4.11 *Weber* concerned the German equivalent of the s. 8(4) Regime, known as "strategic monitoring". For present purposes three features of strategic monitoring are to be noted:

(1) Like the s. 8(4) Regime, strategic monitoring did not involve interception that had to be targeted at a specific individual or premises (see §4 of *Weber*, where

---

112 [***See Annex 26***]

113[***See Annex 11***]

strategic monitoring was distinguished from "*individual monitoring*"; and see the reference to 10% of all telecommunications being potentially subject to strategic monitoring at §110).

(2) Like the s. 8(4) Regime, strategic monitoring involved two stages. In the case of strategic monitoring, the first stage was the interception of wireless communications (§26 of *Weber*) in manner that was not targeted at specific individuals and that might potentially extend to 10% of all communications; and the second stage involved the use of "*catchwords*" (§32). Against this background the applicants in *Weber* complained - as the Claimants do in these proceedings - that the intercepting agency in question was "*entitled to monitor all telecommunications within its reach without any reason or previous suspicion*" (§111).

(3) Despite the above, the applicants' Art. 8 challenge in *Weber* to strategic monitoring was not merely rejected, it was found to be "*manifestly ill-founded*" (§§137-138) and thus inadmissible.

4.12 It follows that from the standpoint of the ECHR there is nothing in principle objectionable about:

(1) an interception regime for external communications that is not targeted at specific individuals or premises; or

(2) a two-stage interception regime for external communications that involves an initial interception stage which may in principle lead to a substantial volume of intercepted material being obtained, followed by a selection stage which serves to identify a subset of that material that can thereafter be examined.

This is unsurprising, not least given the points about the practical necessity of the s.8(4) Regime already made above.

4.13 As to *Liberty*:

(1) The statutory predecessor of the s. 8(4) regime (in the Interception of Communications Act 1985) was found not to be "*in accordance with the law*" in *Liberty*. However, the reason for this conclusion was that, at the relevant time,

the UK Government had not published any further details of the interception regime, in the form of a Code of Practice (see §69). In particular, the ECtHR alluded to the type of details that the German authorities considered it safe to publish about the operation of the G10 Act, under consideration in *Weber;* and noted in this regard that the Code under RIPA (that had been published by the time of the ECtHR's judgment) showed that "*it is possible for a State to make public certain details about the operation of a scheme of external surveillance without compromising national security.*" (§68, emphasis added.)

(2) The s. 8(4) regime does not, of course, suffer from this flaw. The Code to which the ECtHR expressly made reference in §68 of *Liberty* remains in force. Indeed, it has been strengthened following *Liberty* by the changes made in January 2016.

4.14 The Applicants are thus plainly wrong to assert that the position remains the same as in *Liberty* and that the IPT misinterpreted the decision in *Liberty*[114]. On the contrary, there is an entirely new statutory regime in place, together with a Code which contains a large number of significant safeguards that were absent from the regime under consideration in *Liberty;* which are directly material to the protection of individuals whose communications may be intercepted pursuant to a s.8(4) warrant; and which the Applicants ignore.

4.15 Further, the Court in *Liberty* did not conclude that Art. 8 required the UK Government to publish the detail of the Secretary of State's "*arrangements*" under s. 6 of the Interception of Communications Act 1985 (now ss. 15-16 of RIPA). Rather, it implicitly accepted that publication of full (rather than "certain") details would be likely to compromise national security. And since the Code reflects the Disclosure, it contains all of those parts of the Intelligence Services' internal arrangements which the IPT considered in the Liberty proceedings could safely be disclosed without damaging national security.

4.16 In *Kennedy* the ECtHR unanimously upheld the Art. 8-compatility of the RIPA regime regarding s. 8(1) warrants. There are, of course, certain differences between that regime and the s. 8(4) Regime. However, there is also much that is similar, or

[114] See Applicants' Additional Submissions at §§49-54.

identical. Thus *Kennedy* affords considerable assistance when considering the specific safeguards listed in §95 of *Weber*. Indeed, the Code has been significantly strengthened since *Kennedy*, including by the addition of provisions to strengthen the s.8(4) Regime safeguards in particular: so the fact that the ECtHR gave the RIPA regime the stamp of approval in *Kennedy* regarding s.8(1) warrants is a strong indicator that the same outcome should follow for the s.8(4) Regime.

iv. *Digital Rights Ireland* is irrelevant

4.17 The Applicants place some reliance upon the judgment of the CJEU in *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and others C-293/12*, 2014/C 175/07, 8 April 2014[115] (See Annex 16). On a proper analysis, the *Digital Rights Ireland* judgment does not affect the approach or conclusions set out above at all. That analysis is supported by the Court of Appeal's reasoning in *R(Davis and Watson) v Secretary of State for the Home Department* [2016] 1 CMLR 48 (See Annex 17).

4.18 *Digital Rights Ireland* was a preliminary reference concerning the validity of Directive 2006/24/EC on Data Retention (See Annex 48), and EU-wide harmonisation measure adopted pursuant to Article 95 EC. The Directive sought to harmonise divergent data retention measures adopted by the Member States under Article 15(1) of Directive 2002/58/EC (See Annex 49)following the terrorist attacks of 11 September 2001 in New York, 11 March 2004 in Madrid, and 7 July 2005 in London. It did this by requiring CSPs in the EU to retain all customer data for a period of not less than 6 months, and up to 2 years, so that it could be made available to law enforcement authorities. The Directive contained no substantive safeguards at all circumscribing access to or use of that communications data.

4.19 As the CJEU had already made clear in its judgment in *Ireland v European Parliament and Council C-301/06*[116], the provisions of Directive 2006/24/EC were *"essentially limited to the activities of service providers"* and did not *"govern access to data or the use*

[115] See the Additional Submissions on the Facts and the Law at §§66-67.
[116] [***See Annex 50***]

thereof by the police or judicial authorities of the Member States"[117]. Directive 2006/24/EC, as a pre-Lisbon Treaty instrument with its legal base in Article 95 EC, concerning the harmonisation of internal market measures[118], could not include substantive rules relating to access to, or use of, data by national law enforcement authorities.

4.20 In its judgment in *Digital Rights Ireland* concerning the validity of that Directive, the CJEU was therefore not concerned with a national regime or any provision governing access to, or use of, retained data by national law enforcement authorities. The issue before the CJEU was that identified by the Advocate General, namely: *"whether the European Union may lay down a measure such as the obligation to collect and retain, over the long term, the data at issue without at the same time regulating it with guarantees on the conditions to which access and use of those data are to be subject, at least in the form of principles…"*[119]

4.21 In answering that question, the CJEU concluded that the EU legislature was not entitled to adopt the wholesale retention regime laid down in Directive 2006/24/EC without including any safeguards in relation to conditions for access. The CJEU went on to find that Directive 2006/24/EC did not contain any such guarantees, in light of the matters set out at §§56-68 of the judgment[120], and that, by adopting the Directive,

[117] See §§80-82 of the judgment.
[118] Article 95(1) EC provided that "*the Council is to adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market*".
[119] See the Opinion of Advocate General Cruz Villalon, *Digital Rights Ireland,* §121. See also §54 of the CJEU's judgment.
[120] The CJEU made observations at §§56-68 in relation to the following matters:
(1) The broad scope of the data retention envisaged under the Directive (§§56-59);
(2) The absence of any provisions in the Directive defining the limits on access to, and subsequent use of, retained data by national authorities, and in particular the absence of any requirement that access to retained data be dependent on a prior review carried out by a court or independent administrative body (§§60-62);
(3) The length of the data retention period provided for under the Directive, and the absence of any statement that the period of retention had to be based on objective criteria (§§63-64);
(4) The absence of specific rules adapted to the quantity of data whose retention was required, the sensitivity of the data, and the risk of unlawful access to those data; and the absence of any obligation on Member States to establish such rules (§66);
(5) The failure to ensure that a particularly high level of protection and security was applied by service providers, in particular by permitting service providers to have regard to economic considerations when determining the level of security and by failing to ensure the irreversible destruction of the data at the end of the retention period (§67);
(6) The lack of any requirement that data be retained within the EU, with the result that oversight by an independent authority of compliance with the requirements of protection and security could not be fully ensured (§68).

the EU legislature had exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the EU Charter[121].

4.22 The CJEU cannot have intended at §§56-68 of the judgment to lay down a definitive set of requirements that must be incorporated into any data retention regime (still less, access regime) adopted by any Member State of the EU, no matter what other checks, balances or safeguards it already has. On a proper analysis, the *Digital Rights Ireland* judgment does not lay down any minimum requirements for access to or retention of data, nor purports to depart from established principles of ECtHR case law.

4.23 **First**, the case was solely concerned with the validity of Directive 2006/24/EC, which, as the CJEU had already established in *Ireland v Parliament*, did not regulate the activities of national law enforcement authorities. The CJEU had no evidence on which to reach a view about the proportionality of the specific safeguards adopted by any individual Member State to protect personal data against the risk of unlawful access, and did not consider the extent to which matters concerning access to data by national policing or security bodies (and safeguards in relation to such matters) were not subject to EU law. So, in identifying at §§56-68 the type of safeguards that were absent from the EU regime, the CJEU was plainly not deciding that those specific safeguards must, as a matter of EU law, be included in any national data retention or access regime.

4.24 **Secondly**, the judgment does not lay down mandatory requirements for access to or retention of data. EU law does not regulate the ability of national police forces or other law enforcement bodies to access or use personal data (save in the very specific context of EU cross-border cooperation in criminal matters[122]). If the CJEU's judgment were to be read as laying down mandatory requirements for national data

[121] Articles 7, 8 and 52(1) of the Charter provide, as far as material:
"7. Everyone has the right to respect for his or her private and family life, home and communications.
8. (1) Everyone has the right to the protection of personal data concerning him or her…
52 (1) Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may only be made if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."
[122] See Council Framework Decision 2008/977/JHA.

access, it would involve the CJEU legislating in relation to national rules, where such rules are not implementing EU law and where there is no EU law basis for imposing such requirements; and moreover doing so in any area where the EU Treaties specifically recognise the Member States' essential interests and responsibilities[123].

4.25 **Thirdly**, the CJEU has repeatedly confirmed that Article 7 of the Charter must be given the same meaning and scope as Article 8(1) ECHR, as interpreted by the ECtHR[124]. Indeed, where a Charter right corresponds to a right guaranteed by the ECHR, as Articles 7 and 8 both do (data protection being an inherent aspect of the right to respect for private life), Article 52(3) of the Charter requires that the meaning and scope of the rights under the ECHR and the Charter be the same.

4.26 If the CJEU had intended §§56-68 of its judgment to represent a definitive set of requirements for national access/retention regimes, irrespective of what safeguards and access conditions they already contain, that would have represented a clear and radical departure from the principles established by the ECtHR under Article 8 ECHR, as set out below at §§4.32-4.38.

4.27 However, nothing in the CJEU's judgment indicates that it intended to go beyond, expand, or in any way qualify the established principles in the ECtHR's case law on Article 8 ECHR in its application of the Charter. On the contrary, both the Advocate General and the CJEU referred to, and purported to apply, the ECtHR's case law on Article 8 ECHR: see the judgment at §§35, 47, 54, 55. Indeed, the Advocate General expressly referred to the need to "*remain faithful to the approach of the case-law of the European Court of Human Rights*"[125]

4.28 The Court of Appeal in *Davis and Watson*[126] has recently addressed whether the CJEU intended in *Digital Rights Ireland* to lay down definitive mandatory requirements for national regimes concerning the retention of communications data. Mr Davis and Mr

[123] See in particular Article 4(2) of the Treaty on the European Union, which requires the EU to respect Member States' essential State functions, including ensuring territorial integrity, maintaining law and order, and safeguarding national security, the latter of which remains the sole responsibility of each Member State.
[124] See e.g. *McB v Ireland C-400/10* at §53
[125] See the Advocate-General's Opinion at §110.
[126] See [***Annex 17***]

Watson (Members of the UK Parliament) challenged the legality of the Data Retention and Investigatory Powers Act 2014 ("DRIPA"), an Act of Parliament providing for the retention of communications data by communications providers, pursuant to a retention notice served by the Secretary of State. They asserted that DRIPA was inconsistent with EU data protection law on the basis of *Digital Rights Ireland,* which (they said) laid down mandatory requirements for a national retention regime. The Court of Appeal reached the provisional conclusion at §106 of the judgment – essentially, on the basis of the matters set out above – that *Digital Rights Ireland* did not lay down such mandatory requirements, but was concerned simply with the validity of Directive 2006/24/EC. However, the Court of Appeal referred the issue to the CJEU on the basis that it was not *acte clair*. So the CJEU will shortly be reconsidering the effect of its conclusions in *Digital Rights Ireland*.

v. Intercepting communications is in general more intrusive than obtaining communications data

4.29 The Court recognised in §84 of *Malone* that it is less intrusive to obtain communications data than the contents of communications. This remains the case even in relation to internet-based communications. For instance, obtaining the information contained in the "to" and "from" fields of an email (*i.e.* who the email is sent to, and who the email is sent by) will generally involve much less intrusion into the privacy rights of those communicating than obtaining the message content in the body of that email.

4.30 The Claimants appear to dispute this, in particular by reference to the possibility of aggregating communications data eg. to build databases or 'datasets'. It is by no means inevitable that aggregating communications data will yield information of any particular sensitivity. For instance, and to take a hypothetical example, the date, time and duration of telephone calls between an employee and his or her office are unlikely to reveal anything particularly private or sensitive, even if the aggregated communications data in question span many months, or even years.

4.31 Nevertheless, it is possible that aggregating communications data may in certain circumstances (and, potentially, with the addition of further information that is not

communications data) yield information that is more sensitive and private than the information contained in any given individual item of communications data. However, it is important to compare like with like. The issue is not whether *e.g.* 50 or 100 items of communications data relating to Syria-based C might - when aggregated - generate more privacy concerns that an intercepted communication sent or received by C. If aggregation is to be considered, then the comparison must be between 50 or 100 items of communications data relating to C and the content of 50 or 100 of C's communications. When the comparison is undertaken on a like-for-like basis, it is clear that §84 of *Malone* remains correct, even in an age of internet-based communications. In particular, the content of communications continues to be generally more sensitive than the communications data that relates to those communications, and that is as true for aggregated sets of information as for individual items of information.

The s.8(4) Regime is "in accordance with the law"

4.32 The Art. 8 interferences in question have a *basis in domestic law*, namely the s. 8(4) Regime. Further, the "*accessibility*" requirement is satisfied in that RIPA is primary legislation[127] and the Code is a public document, and insofar as the operation of the s. 8(4) Regime is further clarified by the Commissioner's Reports, those are also public documents.

4.33 As regards the foreseeability requirement, account must be taken - as in the case of the Intelligence Sharing Regime - of the special context of secret surveillance, and the well-established principle that the requirement of foreseeability "*...cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly.*" (*Weber*, at §93. See also *e.g.* §67 of *Malone*.)

4.34 This fundamental principle applies both to the interception of communications (so as to obtain intercepted material, *i.e.* the content of communications) and to the obtaining of related communications data (*i.e.* data that does not include the content

[127] Insofar as the s.8(4) Regime incorporates parts of the Intelligence Sharing and Handling regime, that also is "accessible".

of any communications). However, in other respects, the precise requirements of foreseeability differ for the interception of communications, on the one hand, and the obtaining of related communications data, on the other, as the former is more intrusive than the latter (see §§4.57-4.64 above).

Foreseeability of the interception of communications under the s. 8(4) regime

4.35 Subject to the principle set out in §4.33 above, there needs to be clear, detailed rules on the interception of communications to guard against the risk that such secret powers might be exercised arbitrarily (*Weber*, at §§93-94). As has already been noted, the ECtHR has developed the following set of six "*minimum safeguards*" that need to be set out in the domestic legal framework that governs the interception of communications, in order to ensure that the "*foreseeability*" requirement is met in this specific context:

> "*[1] the nature of the offences which may give rise to an interception order; [2] a definition of the categories of people liable to have their telephones tapped; [3] a limit on the duration of telephone tapping; [4] the procedure to be followed for examining, using and storing the data obtained; [5] the precautions to be taken when communicating the data to other parties; and [6] the circumstances in which recordings may or must be erased or the tapes destroyed ...*" (*Weber*, at §95).

4.36 As already noted, *Liberty, Kennedy* and *Zakharov* make clear that it is not necessary that every provision / rule be set out in primary legislation: see §3.33 above.

4.37 §95 of *Weber* applies insofar as the s. 8(4) Regime authorises the interception of communications. First, *Weber* concerned the German equivalent of the s. 8(4) Regime. Secondly, §95 of *Weber* was applied in *Liberty*, which concerned the statutory predecessor to the s. 8(4) Regime. In the light of the above, the various safeguards listed in §95 of *Weber* are addressed - in turn - at §§4.40-4.55 below. Such a point-by-point analysis is a necessary part of determining compliance with the "*in accordance with the law*" requirement for interception: see *e.g.* the ECtHR's approach in §§159-164 of *Kennedy*, and *Weber* itself, at §§96-100. By contrast:

(1) The test is not whether, in one or more respects, the s. 8(4) Regime is somehow broader or less tightly defined then the German strategic monitoring regime at issue in *Weber* (not least because strategic monitoring satisfied the "*in accordance with the law*" requirement by some margin, in that the Art. 8 complaint in *Weber* was thrown out as "*manifestly ill-founded*": §138).

(2) Nor is the test whether the Government might be able to publish some more details of the s. 8(4) Regime or impose at least some more constraints on the powers that are exercised under it.

4.38 As the ECtHR recognised in §95 of *Weber*, the reason why such safeguards need to be in a form accessible to the public is in order to avoid "*abuses of power*". This requirement is thus a facet of the more general principle that there must be adequate and effective guarantees against abuse. Accordingly, in determining whether the domestic safeguards meet the minimum standards set out in §95 of *Weber*, account should be taken of all the relevant circumstances, including: "*the authorities competent to ... supervise [the measures in question], and the kind of remedy provided by the national law ...*" (*Association for European Integration and Human Rights v. Bulgaria*, Appl. no. 62540/00, 28 June 2007, at §77.)

4.39 Thus, as in the case of the Intelligence Sharing and Handling Regime, the Government relies on the relevant oversight mechanisms, namely the Commissioner, the ISC and the Tribunal. The Government emphasises the following points:

(1) The Commissioner has himself stated that his investigations are "*thorough and penetrating*" and that he has "*no hesitation in challenging the public authorities wherever this has been necessary*" (2013 Annual Report at §6.3.3[128]). As to his powers to compel disclosure / the provision of documents and information, the Commissioner has found "*that everyone does this without inhibition*" and that he is thus "*fully informed, or able to make [himself] fully informed about all interception ... activities ... however sensitive these may be*" (2013 Annual Report at §2.14).[129]

(2) The Commissioner regularly inspects the Intelligence Services and the work

[128] See ***[Annex 11]***
[129] See also §§6.1.1-6.1.2 of the Commissioner's 2013 Annual Report.

of senior officials and staff at the relevant Departments of State, and produces "*detailed*" written reports and recommendations (Mr Farr §§87-95). He also is empowered to investigate individual matters of concern, should he consider it appropriate to do so (see Sections 5-6 of the 2013 Annual Report[130]).

(3) Whilst the full details of the ss. 15 and 16 safeguards cannot safely be put into the public domain (Farr §100), (i) the Commissioner is required to keep them under review (s. 57(2)(d)(i) of RIPA), (ii) any breach of them must be reported to him (§7.1 of the Code) and (iii) in practice his advice is sought when any substantive change is proposed (Mr Farr §104).

(4) The ISC has given detailed and penetrating consideration to the s.8(4) Regime in the ISC Report.

(5) As regards the Tribunal, a claimant does not need to be able to adduce cogent evidence that some steps have in fact been taken by the Intelligence Services in relation to him before his claim will be investigated. As a result of that test, the applicants were able to challenge the s.8(4) Regime in the Liberty proceedings, and the Tribunal fully investigated the regime in those proceedings.

(1) The "offences" which may give rise to an interception order

4.40 This requirement is satisfied by s. 5 of RIPA, as read with the relevant definitions in s.81 of RIPA and §§6.11-6.12 of the Code. This follows, in particular, from a straightforward application of §159 of *Kennedy*, and §133 of *RE v United Kingdom*. (See further below at §§4.77-4.81 as regards the meaning of "national security").

(2) The categories of people liable to have their 'telephones tapped'

4.41 As is clear from §97 of *Weber*, this second requirement in §95 of *Weber* applies <u>both</u> to the interception stage (which merely results in the obtaining / recording of communications) and to the subsequent selection stage (which results in a smaller volume of intercepted material being read, looked at or listened to by one or more persons).

[130] See ***[Annex 11]***

4.42 As regards the *interception* stage:

(1) As appears from s. 8(4)(a) and s. 8(5) of RIPA, a s. 8(4) warrant is directed primarily at the interception of external communications.

(2) The term "communication" is sufficiently defined in s. 81 of RIPA. The term "external communication" is sufficiently defined in s. 20 and §5.1 of the Code (see §§4.66-4.76 below). The s. 8(4) regime does not impose any limit on the types of "external communications" at issue, with the result that the broad definition of "communication" in s. 81 applies in full and, in principle, anything that falls within that definition may fall within s. 8(5)(a) insofar as it is "external".

(3) Further, the s. 8(4) regime does not impose any express limit on number of external communications which may fall within "the description of communications to which the warrant relates" in s. 8(4)(a). As is made clear in numerous public documents, a s. 8(4) warrant may in principle result in the interception of "substantial quantities of communications…contained in "bearers" carrying communications to many countries"[131]. Similarly, during the Parliamentary debate on the Bill that was to become RIPA, Lord Bassam referred to intercepting the whole of a communications "link" (see §1.37 above).

(4) In addition, a s. 8(4) warrant may in principle authorise the interception of internal communications insofar as that is necessary in order to intercept the external communications to which the s. 8(4) warrant relates. See s. 5(6) of RIPA, and the reference back to s. 5(6) in s. 8(5)(b) of RIPA (which latter provision needs to be read with s. 8(4)(a) of RIPA). This point was also made clear to Parliament (see §1.37 above) and it has in any event been publicly confirmed by the Commissioner (see §1.39 above).

(5) In the circumstances, and given that an individual should not be enabled "*to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly*" (see §4.33 above) and in the light of the available oversight mechanisms (see §§2.105-2.124 above), the s. 8(4) regime sufficiently identifies the categories of people who are liable to have their communications intercepted.

[131] See the 5 December Judgment at §93. See too, for example, the ISC Report.

4.43 As regards the *selection* stage:

(1) No intercepted material will be read, looked at or listened to by any person unless it falls within the terms of the Secretary of State's certificate, and unless (given s. 6(1) HRA) it is proportionate to do so in the particular circumstances of the case.

(2) As regards the former, material will only fall within the terms of the certificate insofar as it is of a category described therein; and insofar as the examination of it is necessary on the grounds in s. 5(3)(a)-(c) RIPA. Those grounds are themselves sufficiently defined for the purposes of the foreseeability requirement. See §159 of *Kennedy* (and see also *mutatis mutandis* §160 of *Kennedy*: "*there is an overlap between the condition that the categories of person be set out and the condition that the nature of the offences be clearly defined*"). See further at §§4.77-4.81 below as regards the meaning of "national security".

(3) Further, s. 16(2) RIPA, as read with the exceptions in s. 16(3)-(5A), place sufficiently precise limits on the extent to which intercepted material can be selected to be read, looked at or listened to according to a factor which is (a) referable to an individual who is known to be for the time being in the British Islands and (b) which has as its purpose, or one of its purposes, the identification of material contained in communications sent by him or intended for him.

(4) As found by the IPT "referable to" (s. 16(2)(a)) is a wide term and generally accepted to be so as a matter of statutory construction. It would prohibit the use of terms which were connected with, or could lead to the identity of, the individual by the use of names, nicknames, addresses, descriptions or other similar methods (see §104 of the 5 December judgment in the *Privacy* proceedings). If the term was any more specific then it would become unworkable. In those circumstances the criticisms of this term at §46(3)(a) of the Applicants' Additional Submissions are misplaced).

(5) Thus, by way of example, intercepted material could not in general be selected to be listened to by reference to a UK telephone number. Before this could be done, it would be necessary for the Secretary of State to certify that

the examination of a person's communications by reference to such a factor was necessary; any such certification would need to reflect the NSC's "Priorities for Intelligence Collection"[132].

(6) As to the suggestion that the term "*known to be* for the time being in the British Islands" (s. 16(2)(a)) does not prevent inspection where there is a "strong suspicion" that the person is in the UK (see §46(3)(b) of the Applicants' Additional Submissions), the latter would clearly pose too high a hurdle, particularly in the course of extended examination of substantial numbers of communications, as found by the IPT at §104 of the 5 December judgment in the *Privacy* proceedings

(7) In addition, the condition at s. 16(2)(b) is not too limited a restriction[133] in circumstances where the aim is to prevent access to communications sent by or sent to an individual who is in the United Kingdom; see the final sentence of §104 of the 5 December judgment in the *Privacy* proceedings.

4.44 The applicants contend that the safeguards in s.16(2) can be "swept aside" by the "wide discretion" given to the Secretary of State under s.16(3) (which provides for strictly limited circumstances in which it is permissible to select intercepted material by reference to factors which satisfy ss. 16(2)(a) and 16(2)(b) – see §2.74 above). That is wrong. The Secretary of State's power to modify a certificate under s. 16(3) so that intercepted material can be selected according to a factor that is referable to a particular identified individual is in substance as tightly constrained as his power to issue a s. 8(1) warrant, the ECHR-compatibility of which was confirmed by the ECtHR in *Kennedy*.

4.45 In addition, it is well established as a matter of domestic law that an authority must discharge its functions so as to promote – and not so as to thwart or act contrary to – the policy and objects of the legislation conferring the powers in question (see *Padfield v Minister of Agriculture Fisheries and Food* [1968] AC 997 and in particular the speech of Lord Reid at p.1030B-D, p.1033A, and p.1045G). Hence it is wrong to

[132] See the Code, §6.14. In addition guidance is given as to how the Secretary of State will assess such necessity: See §7.19 of the Code.
[133] Contrary to the submissions made at 46(3)(c) of the Applicants' Additional Submissions.

suggest [134] that the Intelligence Services could deliberately circumvent the requirements of s.16(2) by taking action where a person was living in the UK but was known to be out of the UK for a short period. That would be to deliberately undermine the policy objectives of the legislation and would be unlawful as a matter of domestic public law.

4.46 These controls in s.16 RIPA (and the HRA) constrain all access at the selection stage, irrespective whether such access is requested by a foreign intelligence partner. Further, any such access requested by a foreign partner, as it would amount to a disclosure by the Intelligence Service in question to another person, would similarly have to comply with s. 6(1) of the HRA and be subject to the constraints in ss. 1-2 of the SSA and ss. 1-2 and 3-4 of the ISA, as read with ss. 19(3)-(5) of the CTA.

4.47 The regime thus does not permit indiscriminate trawling, as the Commissioner has publicly confirmed (see his 2013 Annual Report at §6.5.43).

4.48 In the light of the above and, having regard - again - to the principle that an individual should not be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly and to the available oversight mechanisms, the s. 8(4) regime sufficiently identifies the categories of people who are liable to have their communications read, looked at or listened to by one or more persons. The IPT was right so to conclude in the *Liberty* proceedings.

(3) Limits on the duration of 'telephone tapping'

4.49 The s. 8(4) Regime makes sufficient provision for the duration of any s.8(4) warrant, and for the circumstances in which such a warrant may be renewed: see §§2.82-2.85 above, §161 of *Kennedy*, and the specific provisions for renewal of a warrant contained in §§6.22-6.24 of the Code[135].

[134] See §46(5) of the Applicants' Additional Submissions.
[135] Note too that the provisions for renewal of a warrant contained in §§6.22-6.24 of the Code are at least as detailed as those found lawful by the ECtHR in relation to the renewal of warrants for covert surveillance under Part II RIPA, considered in *RE v United Kingdom*: see *RE* at §137. Contrast §162 of

4.50 The possibility that a s. 8(4) warrant might be renewed does not alter the analysis. If, in all the circumstances, a s. 8(4) interception warrant continues to be necessary and proportionate under s. 5 of RIPA each time it comes up for renewal, then the Secretary of State may lawfully renew it. The Strasbourg test does not preclude this. Rather, the test is whether there are statutory limits on the operation of warrants, once issued. There are such limits here.

(4)-(5) The procedure to be followed for examining, using and storing the data obtained; and the precautions to be taken when communicating the data to other parties

4.51 Insofar as the intercepted material cannot be read, looked at or listened to by a person pursuant to s.16 (and the certificate in question), it is clear that it cannot be used at all. Prior to its destruction, it must of course be securely stored (§7.7 of the Code).

4.52 As regards the intercepted material that can be read, looked at or listened to pursuant to s.16 (and the certificate in question), the applicable regime (see §§2.69-2.81 above) is well sufficient to satisfy the fourth and fifth foreseeability requirement in §95 of *Weber*. See §163 of *Kennedy*, and the following matters (various of which add to the safeguards considered in *Kennedy*):

(1) Material must generally be selected for possible examination, applying search terms, by equipment operating automatically for that purpose (so that the possibility of human error or deliberate contravention of the conditions for access at this point is minimised). Moreover, before any material can be examined at all, the person examining it must create a record setting out why access to the material is required and proportionate, and consistent with the applicable certificate, and stating any circumstances that are likely to give rise to a degree of collateral infringement of privacy, and any measures taken to reduce the extent of that intrusion. See Code, §§7.14-7.16.

---

the Application, which wrongly states that chapter 6 of the Code does not *"impose any limits on the scope or duration of warrants"*.

(2) The Code affords further protections to material examined under the s.8(4) Regime at §§7.11-7.20 (see §§2.79 above). Thus, material should only be examined by authorised persons receiving regular training in the operation of s.16 RIPA and the requirements of necessity and proportionality; systems should to the extent possible prevent access to material without the record required by §7.16 of the Code having been created; the record must be retained for the purposes of subsequent audit; access to the material must be limited to a defined period of time; if access is renewed, the record must be updated with the reasons for renewal; systems must ensure that if a request for renewal of access is not made within the defined period, no further access will be granted; and regular audits, including checks of the particular matters set out in the Code, should be carried out to ensure that the requirements in s.16 RIPA are met.

(3) Material can be used by the Intelligence Services only in accordance with s. 19(2) of the CTA, as read with the statutory definition of the Intelligence Services' functions (in s. 1 of the SSA and ss. 1 and 3 of the ISA) and only insofar as that is proportionate under s. 6(1) of the HRA. See also §7.6 of the Code as regards copying and §7.7 of the Code as regards storage (the latter being reinforced by the seventh data protection principle).

(4) Further, s. 15(2) sets out the precautions to be taken when communicating intercepted material that can be read, looked at or listened to pursuant to s. 16 to other persons (including foreign intelligence agencies: see §3.109 above). These precautions serve to ensure *e.g.* that only so much of any intercepted material or related communications data as is "*necessary*" for the authorised purposes (as defined in s. 15(4)) is disclosed. The s. 15 safeguards are supplemented in this regard by §§7.4 and 7.5 of the Code (see §2.92 above). In addition, any such disclosure must satisfy the constraints imposed by ss. 1-2 of the SSA and ss. 1-2 and 3-4 of the ISA, as read with ss. 19(3)-(5) of the CTA and s. 6(1) of the HRA. Further, and as in the case of the Intelligence Sharing and Handling Regime, disclosure in breach of the "arrangements" for which provision is made in s. 2(2)(a) of the SSA and ss. 2(2)(a) and 4(2)(a) of the ISA is rendered criminal by s. 1(1) of the OSA.

4.53 As already noted, the detail of the s. 15 and s.16 arrangements is kept under review by the Commissioner (see §§2.80-2.81 and §§2.97-2.98 above).

(6) The circumstances in which recordings may or must be erased or the tapes destroyed

4.54 Section 15(3) of RIPA and §§7.8-7.9 of the Code (including the obligation to review retention at appropriate intervals, and the specification of maximum retention periods for different categories of material, which should normally be no longer than 2 years) make sufficient provision for this purpose. See *Kennedy* at §§164-165 (and note that further safeguards in §7.9 of the Code, including the specification of maximum retention periods, have been added to the Code since *Kennedy*). Both s. 15(3) and the Code are reinforced by the fifth data protection principle: see §2.16 above.

4.55 Further there is no merit in the criticism at §47 of the Applicants' Additional Submissions that the destruction provisions in s.15(3) are undermined by the requirement in s.15(4) to retain material where that is necessary for the authorised purposes. The extreme scenario posited in §47 of the Applicants' submissions i.e. a database or dataset where vast quantities of communications and communications data are retained indefinitely, would be contrary to the maximum retention periods spelt out at §7.9 of the Code and would clearly fail to satisfy the requirements of necessity and proportionality if, exceptionally, data is to be held for longer than those periods (see §7.9 of the Code).

Conclusion as regards the interception of communications

4.56 It follows that the s. 8(4) regime provides a sufficient public indication of the safeguards set out in §95 of *Weber*. As this is all that "foreseeability" requires in the present context (see §§95-102 of *Weber*), it follows that the s. 8(4) regime is sufficiently "*foreseeable*" for the purposes of the "*in accordance with the law*" requirement in Art. 8(2). The IPT was right so to conclude in the *Liberty* proceedings.

Foreseeability of the acquisition of related communications data under the s. 8(4)

Regime

4.57 *Weber* concerned the interception of the content of communications as opposed to the acquisition of communications data as part of an interception operation (see §93 of *Weber*). So far as the Respondents are aware, the list of safeguards in §95 of *Weber* (or similar lists in the other recent ECtHR interception cases) has never been applied by the ECtHR to powers to acquire communications data. This is not surprising. As has already been noted, the covert acquisition of communications data is considered by the ECtHR to be less intrusive in Art. 8 terms than the covert acquisition of the content of communications, and that remains true in the internet age. Thus, as a matter of principle, it is to be expected that the foreseeability requirement will be somewhat less onerous for covert powers to obtain communications data than for covert powers to intercept the content of communications.

4.58 Moreover, the ECtHR has specifically not applied the *Weber* requirements to other types of surveillance. For example, in *Uzun v Germany* app. No. 35623/05, 2 September 2010, the ECtHR specifically declined to apply the "rather strict" standards in *Weber* to surveillance via GPS installed in a suspect's car, which tracked his movements[136]. That sort of tracking information is precisely analogous to the type of information obtained from traffic data (i.e. obtained from a subset of related communications data). Thus, the fact that the Court has declined to apply *Weber* in such circumstances is a powerful indicator that the *Weber* criteria should not apply to the acquisition of related communications data under the s.8(4) Regime.

4.59 Instead of the list of specific safeguards in *e.g.* §95 of *Weber*, the test should therefore be the general one whether the law indicates the scope of any discretion and the manner of its exercise with sufficient clarity "*to give the individual adequate protection against arbitrary interference*" (*Malone* at §68; *Bykov v. Russia* at §78), subject always to

[136] See *Uzun* at §66:
"While the Court is not barred from gaining inspiration from [the Weber criteria], it finds that these rather strict standards, set up and applied in the specific context of surveillance of telecommunications, are not applicable as such to cases such as the present one, concerning surveillance via GPS of movements in public places and thus a measure which must be considered to interfere less with the private life of the person concerned than the interception of his or her telephone conversations. It will therefore apply the more general principles on adequate protection against arbitrary interference with art.8 rights as summarised above."

the critical principle that the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to obtain, access and use his communications data so that he can adapt his conduct accordingly (*c.f.* §93 of *Weber*, and §67 of *Malone*).

4.60 The s. 8(4) Regime satisfies this test as regards the obtaining of related communications data:

(1) As a preliminary point, the controls within the s.8(4) Regime for "related communications data" - as opposed to content - apply to only a limited subset of metadata. "Related communications data" for the purposes of the s.8(4) Regime has the statutory meaning given to it by ss.20 and 21 RIPA[137]. That meaning is not synonymous with, and is significantly narrower than, the term "metadata", used by the Applicants in this context. The Applicants define "metadata" as "*structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource*" (see Application, §21). On that definition, much "metadata" amounts to the content of communications for the purposes of the s.8(4) Regime, not related communications data (since all information that is not "related communications data" must be treated as content). For instance, if a processing system was able to extract or generate a structured index of the contents of a communication, it would be "metadata"; but would be content for

[137] By section 20 RIPA: *""Related communications data", in relation to a communication intercepted in the course of its transmission by means of a postal service or telecommunication system, means so much of any communications data (within the meaning of Chapter II of this Part) as-*

(a) Is obtained by, or in connection with, the interception; and
(b) Relates to the communication or to the sender or recipient, or intended recipient, of the communication".

By section 21(4) RIPA:
"In this Chapter "communications data" means any of the following-

(a) Any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted;
(b) Any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person-
i. Of any postal service or telecommunications service; or
ii. In connection with the provision to or use by any person of any telecommunications service, or any part of a telecommunication system;
(c) Any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service."

the purposes of the s.8(4) Regime. Extracting email addresses or telephone numbers from the body of a communication would generate "metadata"; but would be "content" for the purposes of the s.8(4) Regime. The language or format used for a communication would be "metadata"; but again, "content" for the purposes of the s.8(4) Regime.

(2) The s. 8(4) Regime is sufficiently clear as regards the circumstances in which the Intelligence Services can **obtain** related communications data: see §§4.41-4.43 above, which applies equally here.

(3) Once obtained, **access** to any related communications data must be necessary and proportionate under s. 6(1) of the HRA, and will be subject to the constraints in ss.1-2 of the SSA and ss. 1-2 and 3-4 of the ISA. Any access by any foreign intelligence partner at this stage would be constrained by ss. 15(2)(a) and 15(2)(b) of RIPA (as read with s. 15(4)); and, as it would amount to a disclosure by the Intelligence Service in question to another person would similarly have to comply with s. 6(1) of the HRA and be subject to the constraints in ss. 1-2 of the SSA and ss. 1-2 and 3-4 of the ISA, as read with ss. 19(3)-(5) of the CTA.

(4) Given the constraints in ss. 15 of RIPA and s. 6(1) of the HRA, communications data cannot be used (in combination with other information / intelligence) to discover *e.g.* that a woman of no intelligence interest may be planning an abortion. This is for the simple reason that obtaining this information would very obviously serve none of the authorised purposes in s. 15(4). There is nothing unique about communications data (even when aggregated) here. Other RIPA powers, such as the powers to conduct covert surveillance and the use of covert human intelligence sources, might equally be said to be capable of enabling discovering of the fact that a woman of no intelligence interest may be planning an abortion (*e.g.* an eavesdropping device might be planted in her home, or a covert human intelligence source might be tasked to befriend her). But it is equally clear that these powers could not in practice be used in this way, and for precisely the same reason: such activity would very obviously not be for the relevant statutory purposes (see ss. 28(3), 29(3) and 32(3) of RIPA).

4.61 Further, there is good reason for s. 16 of RIPA covering access to intercepted material (*i.e.* the content of communications) and not covering access to communications data (see the Applicants' complaints at §46(1) of their Additional Submissions):

(1) In order for s. 16 to work as a safeguard in relation to individuals who are within the British Islands, but whose communications might be intercepted as part of the S. 8(4) Regime, the Intelligence Services need information to be able to assess whether any potential target is "*for the time being in the British Islands*" (for the purposes of s. 16(2)(a)). Communications data is a significant resource in this regard.

(2) In other words, an important reason why the Intelligence Services need access to related communications data under the s. 8(4) Regime is precisely so as to ensure that the s. 16 safeguard works properly and, insofar as possible, factors are not used at the selection that are - albeit not to the knowledge of the Intelligence Services - "*referable to an individual who is ... for the time being in the British Islands*".

4.62 The regime equally contains sufficient clear provision regarding the subsequent **handling, use and possible onward disclosure** by the Intelligence Services of related communications data. See, *mutatis mutandis*, §§2.86-3.42 above.

4.63 In the alternative, if the list of safeguards in §95 of *Weber* applies to the obtaining of related communications data, then the s. 8(4) Regime meets each of those requirements so imposed given §§4.40-4.55 above (and, as regards the limits on the duration of s. 8(4) warrants, §§4.49-4.50 above).

4.64 For the reasons set out above, the s.8(4) Regime is sufficiently foreseeable to satisfy the "in accordance with the law" test, both as regards the interception and handling of the content of communications, and as regards the interception and handling of related communications data.

Further issues regarding foreseeability/accessibility

4.65 The Applicants raise certain specific complaints about the foreseeability of the s.8(4) Regime, each of which is addressed below in order to explain why it does not affect the general conclusion on foreseeability/accessibility set out above. They are:

(1) The lack of clarity in the definition of "external communications"[138];

(2) The breadth of the concepts of "national security" and "serious crime" [139].

The definition of "external communications"

4.66 The meaning of an "external communication" for the purposes of Chapter I of RIPA is stated in s. 20 of RIPA to be "a communication sent or received outside the British Islands". That definition is further clarified by §6.5 of the Code:

> "*External communications are defined by RIPA to be those which are sent or received outside the British Islands. They include those which are both sent and received outside the British Islands, whether or not they pass through the British Islands in course of their transmission. They do not include communications both sent and received in the British Islands, even if they pass outside the British Islands en route. For example, an email from a person in London to a person in Birmingham will be an internal, not an external, communication for the purposes of section 20 of RIPA, whether or not it is routed via IP addresses outside the British Islands, because both the sender and intended recipient are within the British Islands.*"

4.67 The Applicants complain at §45 of their Additional Submissions about the lack of any practical distinction between internal and external communications and the lack of clarity in relation to external communications. These complaints are unfounded; (and identical complaints were rejected by the IPT in the Liberty proceedings – see 5 December Judgment, §§93-101):

(1) The definition of an "external communication" is sufficiently clear in the

[138] See Additional Submissions at §45.
[139] See Additional Submissions at §46(2).

circumstances.

(2) Whilst in practice the analysis of whether an individual electronic communication is "internal" or "external" may be a difficult one (which can be conducted only with the benefit of hindsight), this has no bearing upon whether a specific communication is likely to be intercepted under the s. 8(4) Regime. The distinction between "external" and "internal" communications is an important safeguard at a "macro" level (when the Intelligence Services decide which communications bearer to intercept): but that exercise has nothing to do with whether a particular communication is "internal" or "external", applying the definition in s.20 RIPA.

(3) This issue similarly has no bearing on the application of the safeguards in ss. 15 and 16 of RIPA, in the sense that both apply to communications whether or not they are external.

(4) As regards the examination of any intercepted material, the significant protection offered by s. 16(2) does not turn on the definition of external communications, but on the separate concept of a "factor ... referable to an individual who is known to be for the time being in the British Islands".

4.68 **First**, the definition of "external communications" is itself a sufficiently clear one, in the circumstances. It draws a distinction between communications that are both sent and received within the British Islands, and communications that are not both sent and received within the British Islands; and the focus of the definition is upon the ultimate sender, and ultimate intended recipient, of the communication. Thus, for the purposes of determining whether a communication is internal or external it matters not that a particular communication may be handled either by persons or by servers en route, who are located outside the British Islands; what matters is only where the sender and intended recipient of the communication are based: see Mr Farr §§129-130. This position reflects what was stated by Lord Bassam during the passage of RIPA through Parliament (set out at §1.37 above).

4.69 Further, although the ways in which the internet may be used to communicate evolves and expands over time, the application of the definition remains foreseeable. Thus, where the ultimate recipient is *e.g.* a Google web server (in the case of a Google search), the status of the search query - as a communication - will depend on the

location of the server. Further, when a communication in the form of public post or other public message is placed on a web-based platform such as Facebook or Twitter, the communication will be external if the server in question (as the ultimate recipient) is outside the British Islands. By contrast, if such a platform is used to send what is in effect a private message to a particular individual recipient, then - as in the case of a telephone call, or an ordinary email - the status of the communication in question will depend on whether that recipient is within or outside the British Islands. (And the same analysis applies if the private message is sent to a group of individual recipients: as in the case of an ordinary email, the private message will be an internal communication if all recipients are within the British Islands): see Mr Farr §§133-137.[140]

4.70 That said, the nature of electronic communication over the internet means (and has always meant) that the factual analysis whether a particular communication is external or internal may in individual cases be a difficult one, which may only be possible to carry out with the benefit of hindsight. But that is not a question of any lack of clarity in RIPA or the Code: it reflects the nature of internet-based communications. For example, suppose that London-based A emails X at X's Gmail email address. The email will be sent to a Google server, in all probability outside the UK, where it will rest until X logs into his Gmail account to retrieve the email. At the point that X logs into his Google mail account, the transmission of the communication will be completed. If X is located within the British Islands at the time he logs into the Google mail account, the communication will be internal; if X is located outside the British Islands at that time, the communication will be external. Thus it cannot be known for certain whether the communication is in fact external or internal until X retrieves the email; and until X's location when he does so is analysed.

[140] The Applicants imply that the Code should explain how the distinction between "external" and "internal" communications applies to various modern forms of internet use (see e.g. the complaint at §45(2) of the Additional Submissions, that the Code of Practice is *"silent on the status of many forms of modern internet based communications"*. The difficulty with this submission is if it were correct, then each time a new form of internet communication is invented, or at least popularised, the Code would need to be amended, published in draft, and laid before both Houses of Parliament, in order specifically to explain how the distinction applied to the particular type of communication at issue. That would be both impractical and (for reasons explained in §§4.69-4.70) pointless; and the "in accordance with the law" test under Art. 8 cannot conceivably impose such a requirement.

4.71 However, the Applicants wrongly assume that any such difficulties in applying the definition of "*external communication*" to a specific individual communication is relevant to the operation of the s. 8(4) Regime in relation to that communication. It is not:

(1) Whilst a s. 8(4) warrant in principle permits interception of what is (at the point of interception) a substantial volume of communications to be intercepted, it is necessary that the communications actually sought are "external communications" of a particular description, which must be set out in the warrant: see s. 8(4). Further, interception will be targeted at communications "links" (to use Lord Bassam's wording). However, the legislative framework expressly authorises the interception of internal communications not identified in the warrant, to the extent that this is necessary to obtain the "external communications" that are the subject of the warrant: see s. 5(6)(a) RIPA; and (as Lord Bassam explained to Parliament, and given §1.36 above) is in practice inevitable that, when intercepting material at the level of communications links, both "*internal*" and "*external*" communications will be intercepted.

(2) Thus, the distinction between external and internal communications offers an important safeguard at a "macro" level, when it is determined what communications links should be targeted for interception under the s. 8(4) Regime. When deciding whether to sign a warrant under section 8(4) RIPA, the Secretary of State will – indeed must – select communications links for interception on the basis that they are likely to contain external communications of intelligence value, which it is proportionate to intercept. Moreover, interception operations under the s. 8(4) Regime are conducted in such a way that the interception of communications that are not external is kept to the minimum necessary to achieve the objective of intercepting wanted external communications (Mr Farr §154). However, that has nothing to do with the assessment whether, in any specific case, a particular internet-based communication is internal or external, applying the definition of "external communication" in s. 20 of RIPA and the Code.

4.72 In short, how the definition of "external communication" applies to any particular electronic communication is immaterial to the foreseeability of its interception. This is the **second** point.

4.73 **Thirdly**, the safeguards in ss. 15 and 16 (as elaborated in the Code) apply to internal as much as to external communications, and thus the scope of application of these safeguards does not turn on the distinction between these two forms of communication.

4.74 **Fourthly**, it is the safeguard in s. 16(2) that affords significant protections for persons within the British Islands, and this provision does not turn on the definition of external communications, but on the separate concept of a "factor ... referable to an individual who is known to be for the time being in the British Islands".

4.75 For example, London-based person A undertakes a Google search. Such a search would in all probability be an external communication, because it would be a communication between a person in the British Islands and a Google server probably located in the US (see *Farr §134*). Nevertheless, irrespective of whether the communication was external or internal, it could lawfully be intercepted under a section 8(4) warrant which applied to the link carrying the communication, as explained above. However, it could <u>not</u> be examined by reference to a factor relating to A, unless the Secretary of State had certified under section 16(3) RIPA that such examination was necessary, by means of an <u>express</u> modification to the certificate accompanying the section 8(4) warrant.

4.76 For all those reasons, any difference of view between the Applicants and Government as to the precise ambit of the definition of "external communications" in s.20 RIPA does not render the s.8(4) Regime contrary to Article 8(2) ECHR. The IPT was right so to conclude in the Liberty proceedings[141].

<u>The breadth of the concepts of "national security" and "serious crime"</u>

[141] See 5 December Judgment, §101.

4.77 The Applicants complain about what they contend is the excessive breadth of the categories of "national security" and "serious crime" which they say "provides no meaningful restriction on the scope of the intelligence services' discretion to inspect intercepted material": see Additional Submissions at §46(2).

4.78 **First,** the Court has consistently held in a long line of authority that the term "national security" is sufficiently foreseeable to constitute a proper ground for secret surveillance measures, provided that the ambit of the authorities' discretion is otherwise controlled by appropriate and sufficient safeguards. Most notably for present purposes, the applicant in *Kennedy* asserted that the use of the term "national security" as a ground for the issue of a warrant under s.5(3) RIPA was insufficiently foreseeable, just as the Applicants now contend; and that argument was rejected in terms by the Court at §159:

> "*As to the nature of the offences, the Court emphasises that the condition of foreseeability does not require states to set out exhaustively by name the specific offences which may give rise to interception. However, sufficient detail should be provided of the nature of the offences in question. In the case of RIPA, s.5 provides that interception can only take place where the Secretary of State believes that it is necessary in the interests of national security, for the purposes of preventing or detecting serious crime, or for the purposes of safeguarding the economic well-being of the United Kingdom. The applicant criticises the terms "national security" and "serious crime" as being insufficiently clear. The Court disagrees. It observes that the term "national security" is frequently employed in both national and international legislation and constitutes one of the legitimate aims to which art. 8(2) itself refers. The Court has previously emphasised that the requirement of "foreseeability" of the law does not go so far as to compel states to enact legislative provisions listing in detail all conduct that may prompt a decision to deport an individual on "national security" grounds. By the very nature of things, threats to national security may vary in character and may be unanticipated or difficult to define in advance. Similar considerations apply to the use of the term in the context of secret surveillance. Further, additional clarification of how the term is to be applied in practice in the United Kingdom has been provided by the Commissioner, who has indicated that it allows surveillance of activities which threaten the safety or well-being of the state*

and activities which are intended to undermine or overthrow parliamentary democracy by political, industrial or violent means."

4.79 The reasoning of the Court in *Kennedy* is that the term "national security" has sufficient clarity without further definition, since threats to national security may be difficult to define in advance, and the term "national security" is one frequently applied in national and international legislation. That reasoning is unaffected by whether the Commissioner's statement is current. It also reflects a consistent line of Convention case law: see e.g. the admissibility decisions in *Esbester v United Kingdom app. 18601/91, Hewitt and Harman v United Kingdom app. 20317/92* and *Campbell Christie v United Kingdom app. 21482/93,* and the recent decision of the ECtHR in *RE v United Kingdom* app. 62498/11 (27 October 2015) at §133.

4.80 Further, the Grand Chamber in *Zakharov* cited §159 of *Kennedy*; reiterated its observation that threats to national security may *"vary in character and be unanticipated or difficult to define in advance"*; and reasoned to the effect that a broad statutory ground for secret surveillance (such as national security) will not necessarily breach the "foreseeability" requirement, provided that sufficient safeguards against arbitrariness exist within the applicable scheme as a whole: see *Zakharov* at §§247-249 and 257[142]. In this case, for all the reasons already set out above at such safeguards plainly exist, both by virtue of the detailed provisions of the Code, and by virtue of the oversight mechanisms of the Commissioner, the ISC and the IPT.

4.81 **Secondly,** the s.8(4) Regime is designed so as to ensure that a person's communications, intercepted under a s.8(4) warrant, cannot be examined simply by reference to unparticularised concerns of "national security". Rather, a specific and concrete justification must be given for each and every access to those communications; and the validity of that justification is subject to internal and external oversight. So the regime contains adequate safeguards against abuse by reference to an overbroad or nebulous approach to "national security". In particular:

[142] See too *Szabo and Vissy v Hungary app. 37138/14,* 12 January 2016, at §64 (where the Court stated that it was "not wholly persuaded" by a submission that a reference to "terrorist threats or rescue operations" was unsufficiently foreseeable, "*recalling that the wording of many statutes is not absolutely precise, and that the need to avoid excessive rigidity and to keep pace with changing circumstances means that many laws are inevitably couched in terms which, to a greater or lesser extent, are vague."*)

(1) Communications cannot be examined at all unless it is necessary and proportionate to do so for one for one of the reasons set out in the certificate accompanying the warrant issued by the Secretary of State. Those reasons will be specific ones, which must broadly reflect the NSC's "Priorities for Intelligence Collection": see Code, §6.14. Moreover, the certificate is under the oversight of the Commissioner, who must review any changes to the descriptions of material within it: see Code, §6.14 and §2.63 above.

(2) Before communications are examined at all, a record must be created, setting out why access to the particular communications is required consistent with s.16 RIPA and the appropriate certificate, and why such access is proportionate: see Code, §7.16 and §2.79 above.

(3) The record must be retained, and is subject both to internal audit and to the oversight of the Commissioner (as well as that of the IPT). See Code, §7.18 and §2.79 above.

4.82 **Finally**, in terms of the contention that the meaning of "serious crime" is insufficiently clear, at §159 of *Kennedy* the ECtHR observes that RIPA itself contains a clear definition both of "serious crime" and what is meant by "detecting" serious crime: see s. 81 RIPA.

4.83 In conclusion, for all the above reasons, the s.8(4) Regime is "in accordance with the law" for the purposes of Article 8 ECHR.

The s.8(4) Regime satisfies the "necessity" test

4.84 As to the question whether the s.8(4) Regime is "necessary in a democratic society" (see §§61-69 of the Applicants' Additional Submissions), the Court has consistently recognised that when balancing the interests of a respondent State in protecting its national security through secret surveillance measures against the right to respect for private life, the national authorities enjoy a "fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security": see e.g. *Weber* at §106, *Klass* at §49, *Leander* at §59, *Malone* at §81. Nevertheless, the Court must be satisfied that there are adequate and effective guarantees against

abuse. That assessment depends on all the circumstances of the case, such as the nature, scope and duration of possible measures; the grounds required for ordering them; the authorities competent to authorise, carry out and supervise them; and the kind of remedy provided by the national law: see e.g. *Zakharov* at §232.

4.85 The Fourth Section has recently suggested in *Szabo and Vissy* (while acknowledging that this "represents at first glance a test different from the one prescribed in [Article 8(2)]") that measures of secret surveillance should be "strictly necessary" in two respects: (i) as a general consideration, for the safeguarding of democratic institutions; and (ii) as a particular consideration, for the obtaining of vital intelligence in an individual operation: see *Szabo,* §§72-73. It is submitted that the test previously set out by the Grand Chamber and in the other long-standing cases just referred to is to be preferred. It represents a properly protective set of principles which balance both the possible seriousness of the Article 8 interference with the real benefits to the general community of such surveillance in protecting them against acts of terrorism. Strict necessity as a concept is used expressly in the Covention scheme – indicating that it should not be imported elsewhere; or, if that is permissible at all, then only with the greatest caution. There is no warrant for any stricter test in principle in the present context.

4.86 However, whether viewed through the prism of general necessity, or adopting the test of "strict necessity" in the respects identified in *Szabo,* the s.8(4) Regime satisfies the necessity test.

4.87 **First,** the s.8(4) Regime contains adequate and effective guarantees against abuse for all the reasons already set out above for the purposes of the "in accordance with the law" test. If those guarantees render the regime "in accordance with the law" (as they do), they plainly satisfy the "necessity test" - not least, given the margin of appreciation available to the State in this area.

4.88 Thus, the safeguards ensure that material is not examined by reference to factors referable to an individual in the UK without the Secretary of State's approval; that the criteria for examining intercepted material are precise and focused, and access to it strictly controlled; that intercept does not occur on the basis of an over-broad

definition of national security; that the use of data both by the Intelligence Services and foreign agency counterparts is sufficiently controlled; and that there is proper judicial and other independent oversight.

4.89 **Secondly,** the s.8(4) Regime is indeed strictly necessary, as a general consideration, for the safeguarding of democratic institutions. The Applicants challenge the regime on the basis that GCHQ's "interception each day of millions of e-mails, Google messages and other data concerning internet use" is not proportionate (see eg. §67 of the Applicants' Additional Submissions). But that both factually mischaracterises the operation of the s.8(4) Regime; and ignores the vital point that the interception of a bearer's entire contents is the only way for the Intelligence Services to obtain the external communications they need to examine for national security purposes. They need the "haystack" to find the "needle".

4.90 The first point here is that communications are not intercepted on the basis of "happenstance" (or to put it another way, simply because they can be). The s.8(4) Regime operates on the basis that the Intelligence Services will identify the particular communication links that are most likely to carry "external communications" meeting the descriptions of material certified by the Secretary of State, and will intercept only those links: see the Code, §6.7. Moreover, and as the Code also states:

(1) The Intelligence Services must conduct the interception in ways that limit the collection of non-external communications to the minimum level compatible with the object of intercepting wanted external communications (Code, §6.7).
(2) The Intelligence Services must conduct regular surveys of relevant communication links, to ensure that they are those most likely to be carrying the external communications they need (Code, §6.7).
(3) Any application for a warrant authorising the interception of a particular communications link must explain why interception of that link is necessary and proportionate for one or more of the purposes in s.5(3) RIPA (Code, §6.10).
(4) If an application is made for the warrant's renewal, the application must not only state why interception of the link continues to be proportionate, but must also give an assessment of the intelligence value of material obtained

from the link to date (Code, §6.22).

4.91 If the Intelligence Services were unlawfully intercepting links on the basis of "happenstance", that is something that would be picked up by the Commissioner as part of his survey of warrants and their justification. But the Commissioner has found the opposite: see e.g. his investigation of the s.8(4) Regime in the 2013 Report at §6.5.42 (***See Annex 11***).

4.92 Further, there are technical reasons why it is not possible to find a wanted communication travelling over a communications link without intercepting the entire contents of that link, and interrogating them automatically (if only for a very short period); and the pressing need to obtain external communications travelling over such links in the interests of national security is plain, on the basis of the findings in the ISC and Anderson Reports (see §§1.33-1.35 above).

4.93 Thus, the ISC has explained that bulk interception under the s.8(4) Regime is *"essential"* if the Intelligence Services are to discover threats effectively (see §2.25). That point is borne out by the examples given at Annex 9 to the Anderson Report (see §1.34 above), which record the discovery and/or successful disruption of major national security threats, in circumstances where bulk interception was the only means likely to have produced the desired intelligence. So if the Applicants wish to say that intercepting the contents of a communications link is inherently disproportionate, they must accept as a corollary the real possibility that the Intelligence Services will fail to discover major threats to the UK (such as a terrorist bomb plot, or a plot involving a passenger jet – see e.g. examples 2 and 6 in Annex 9 to the Anderson Report).

4.94 It would be absurd if the case law of the ECtHR required a finding of disproportionality in such circumstances, merely because the whole contents of a communications link are intercepted, even though only a tiny fraction of intercepted communications are ever, and can ever be, selected for potential examination, let alone examined. On a proper analysis, it does not. See/compare *Weber* and §§4.11-4.12 above.

4.95 **Thirdly,** the question of whether surveillance is necessary "*as a particular consideration, for the obtaining of vital intelligence in an individual operation*" (*Szabo* at §73) appears to relate to the facts of interception in a particular case, rather than to the applicable regime as a whole - thus, for example, to the question whether it corresponds to a pressing social need, and is proportionate, to issue a warrant covering a certain communications link. That question does not arise here, where the challenge is to the s.8(4) Regime *in abstracto*. However, at a systemic level, effective safeguards exist to ensure that (i) communications links are only accessed where necessary and proportionate for the purposes in the Secretary of State's certificate, which themselves must follow the intelligence priorities set by the NSC; and (ii) particular communications from those links can only be examined, if their examination is necessary and proportionate for those purposes. Indeed, in the context of bulk interception (which the Court has confirmed is lawful in principle in *Weber*), the test in *Szabo* can only relate to the stage at which communications are selected for examination: and at that stage, for all the reasons set out above, stringent controls are applied under s.8(4) Regime both as a matter of law and of fact to ensure that communications are only examined where it is necessary and proportionate to do so, because of the intelligence they contain.

Prior judicial authorisation of warrants

4.96 The Applicants contend that prior judicial authorisation of warrants is required for the s.8(4) Regime to be comply with Article 8 ECHR: see §68 of the Applicants' Additional Submissions. The Government strongly deny that the Convention requires or should require any such precondition. Just as in *Kennedy*, the extensive oversight mechanisms in the s.8(4) Regime offer sufficient safeguards to render the regime in accordance with the law, without any requirement for independent (still less, judicial) pre-authorisation of warrants.

4.97 **First,** the Court's case law does not require independent authorisation of warrants as a precondition of lawfulness, provided that the applicable regime otherwise contains sufficient safeguards. Given the possibilities for abuse inherent in a regime of secret surveillance, it is on the whole in principle desirable to entrust supervisory control to a judge: but such control may consist of *oversight* after rather than before the event:

see *Klass v Germany*, 6 September 1978, Series A no.28 at §51, *Kennedy* at §167, and most recently, the detailed consideration of the issue in *Szabo and Vissy v Hungary* app.37138/14 (12 January 2016) at §77:

> *"The Court recalls that in Dumitru Popescu (cited above, §§70-73) it expressed the view that either the body issuing authorisations for interception should be independent or there should be control by a judge or an independent body over the issuing body's activity. Accordingly, in this field, control by an independent body, normally a judge with special expertise, should be the rule and substitute solutions the exception, warranting close scrutiny (see Klass and others, cited above, §§42 and 55). The ex ante authorisation of such a measure is not an absolute requirement per se, because where there is extensive post factum judicial oversight, this may counterbalance the shortcomings of the authorisation (see Kennedy, cited above, §167)."* (Emphasis added)

(To the extent that *Iordachi v Moldova* app.25198/02, 10 February 2009 implies at §40 that there must in all cases be independent prior authorisation of warrants for interception, it is inconsistent with the later cases of *Kennedy* and *Szabo*, and cannot stand with the general thrust of the Court's case law.)

4.98 **Secondly,** there is extensive independent (including judicial) *post factum* oversight of secret surveillance under the s.8(4) Regime. The very same observations made by the ECtHR at §167 of *Kennedy*, in which the Court found that the oversight of the IPT compensated for the lack of prior authorisation, apply equally here:

> *"…the Court highlights the extensive jurisdiction of the IPT to examine any complaint of unlawful interception. Unlike in many other domestic systems, any person who suspects that his communications have been or are being intercepted may apply to the IPT. The jurisdiction of the IPT does not, therefore, depend on notification to the interception subject that there has been an interception of his communications. The Court emphasises that the IPT is an independent and impartial body, which has adopted its own rules of procedure. The members of the tribunal must hold or have held high judicial office or be experienced lawyers. In undertaking its examination of complaints by individuals, the IPT has access to closed material*

and has the power to require the Commissioner to provide it with any assistance it thinks fit and the power to order disclosure by those involved in the authorisation and execution of the warrant of all documents it considers relevant. In the event that the IPT finds in the applicant's favour, it can, inter alia, quash any interception order, require destruction of intercept material and order compensation to be paid. The publication of the IPT's legal rulings further enhances the level of scrutiny afforded to secret surveillance activities in the United Kingdom."

4.99 Moreover, the following additional points about the applicable *post factum* independent oversight should also be made:

(1) The IPT is not only in principle but in fact an effective system of oversight in this type of case, as the Liberty proceedings indicate: see §§1.41-1.51 above.
(2) The Commissioner oversees the issue of warrants under the s.8(4) Regime as part of his functions, and looks at a substantial proportion of all individual warrant applications in detail: see §2.111 above.
(3) The ISC also provides an important means of overseeing the s.8(4) Regime as a whole, and specifically investigated the issuing of warrants in the ISC Report (see the report, pp.37-38, [***See Annex 13***]).

Specific criticisms of IPT's Third Judgment (22 June 2015)

4.100 The applicants have made a number of specific criticisms of the IPT's third judgment dated 22 June 2015.

4.101 **First** it is said that the IPT failed to assess the general proportionality of the s. 8(4) regime and that there has been no proper consideration of that issue at the domestic level. But that is contrary to the express wording of the judgment of 22 June 2015 which made clear that the IPT considered proportionality both as it arose specifically in relation to the claimants' communications and as it arose in respect of the s.8(4) regime as a whole (what it referred to as "systemic proportionality") – see judgment at §3. In any event, for the reasons set out at §§4.84-4.95 above, the regime very clearly satisfies the "necessity" test. In that regard it is important that the s.8(4) regime is not one which can properly or accurately be characterised as one of "bulk

interception surveillance", contrary to the applicant's submissions on the third judgment at §§16-17 and for the reasons set out at §§1.19-1.28 above.

4.102 **Secondly** the applicants assert that the individual determinations in favour of two of the human rights organisations (Amnesty International and the Legal Resource Centre) in the Liberty proceedings are evidence that the UK intelligence services have "*deliberately targeted*" the communications of human rights organisations on the basis that they are "*national security targets*" (see §§18-25 of the applicants' submissions on the Third Judgment).

4.103 No such inference can possibly be drawn from the IPT's conclusions. The IPT found that GCHQ had lawfully and proportionately intercepted, and selected for examination, communications from or to particular email addresses associated with Amnesty International and the Legal Resources Centre; but (in the case of Amnesty International) breached its internal retention policy, and (in the case of the Legal Resource Centre) breached its internal policy on selection. The judgment did not reveal whether or not the particular email address or addresses associated with the claimants had themselves been the target of the interception, or whether they had simply been in communication with the target of the interception. Those conclusions do not imply, still less state, that GCHQ "*deliberately targeted the communications of human rights organisations*" or that "*the government deems that human rights NGOs may legitimately be considered "national security targets*[143]*""*. The IPT was self-evidently aware of the necessary tests which had to be satisfied in order to reach its conclusions, it having set out the requirements of the s.8(4) regime in detail in the 5 December 2014 judgment and having repeated its conclusions at §4 of the 22 June judgment (see in particular at §4(i)(a)). Those tests included the requirement that the selection of communications for examination be necessary and proportionate, and that those communications fall into a category set out in the Secretary of State's certificate under s.5 RIPA. Had the Intelligence Agencies been deliberately targeting human rights organisations in an unlawful/indiscriminate way the IPT would have so stated.

[143] See Submissions, §25.

4.104 **Thirdly** the applicants complain that they are unable to understand how the IPT reached the conclusion that there had been lawful and proportionate interception and accessing/selection in the two individual cases (see §§26-30 of their submissions on the Third Judgment). But that is a function of the fact that the IPT is required by Rule 6(1) to carry out its functions in such a way as to ensure that information is not disclosed to an extent or in a manner which would be contrary to the public interest or prejudicial to national security. That was emphasised by the IPT at §13 of its 22 June 2015 judgment where it made clear that the IPT could only provide the essential elements of its determination because to do otherwise would offend that important rule. As is clear from the Art. 6 case law discussed separately in these Observations (See §7.11-7.31), that there can be circumstances in which it is lawful for material to be withheld on eg. national security grounds, without prejudicing the fairness of the proceedings, is well established. Particularly in circumstances where the IPT had the assistance of CTT (acting in the role of special advocate) to represent the interests of the applicants in the closed proceedings, it cannot be said that this renders the proceedings in breach of Art. 6 (which is what appears to be being implied in this part of the applicants' submissions).

4.105 **Fourthly** the applicants assert that there was a failure to address Art. 10 ECHR in the third judgment. But the applicants do not indicate what Art. 10 would have added to the IPT's consideration of the individual cases or the IPT's conclusion that it was lawful and proportionate to intercept/access the material. These submissions appear to be premised on the basis that it would have been unlawful for the Intelligence Agencies to have deliberately targeted the e-mails of human rights organisations and that such deliberate targeting would have been disproportionate under Art. 10 ECHR. But that is not a proper inference which can be drawn from the terms of the 22 June 2015 judgment for the reasons set out above.

4.106 In addition there is no merit in the complaint that the IPT declined to direct the intelligence services to disclose any of their internal guidance concerning the treatment of confidential material of non-government organisations (NGOs) under Art. 10. This is addressed at §§134-135 of the IPT's 5 December judgment. As is evident from that extract from the judgment:

(1) Liberty only sought to raise, at a very late stage of the IPT proceedings (in written submissions dated 17 November 2014), the issue whether there was adequate provision under Art. 10 ECHR for dealing with confidential information in the context of NGO activities ('NGO confidence');

(2) The issue of NGO confidence was not raised when the legal issues were agreed between all parties on 14 February 2014, some 5 months before the open legal issues hearing in July 2014;

(3) The written arguments addressed at the July 2014 hearing had not raised any separate issue under Art. 10 ECHR in respect of NGO confidence.

(4) Liberty had been given ample opportunity to raise the issue, but had not done so.

(5) The IPT concluded that it was far too late (in November 2014) to be seeking to raise the issue, particularly in circumstances where it was being suggested that further disclosure and "considerable" further argument would be necessary to incorporate it into the proceedings at that stage.

4.107 **Fifthly**, the applicants criticise the IPT for failing to make clear whether the "accessing" of Amnesty's communications involved its communications data and/or whether the communications data of the Legal Resource centre was analysed following its selection for examination. But this criticism is misplaced. Had the IPT considered that any communications data pertaining to Amnesty, the Legal Resource Centre, or any other applicant, had been handled unlawfully, it would have said so in its judgment.

4.108 **Finally** the applicants have submitted that the IPT's correction to its judgment, in which it substituted Amnesty for the Egyptian Initiative for Personal Rights "undermines the Tribunal's earlier findings that the UK surveillance regime contains adequate safeguards to protect fundamental rights". These submissions are not understood. The IPT made clear in its letter dated 1 July 2015 that there had been a mistaken attribution in the judgment which did not result from any failure by the Respondents to make disclosure. That is not a matter which can appropriately lead to the criticism that it demonstrates a lack of rigour in the Tribunal's proportionality assessment. The IPT's judgment (including its proportionality assessment) was

reached after full consideration of the relevant material in closed sessions, where the applicants' interests were represented by CTT, acting in effect as a special advocate.

5 **QUESTION 3. ARTICLE 8 - IMPACT OF THE FACT THAT APPLICANTS ARE NON-GOVERNMENTAL ORGANISATIONS ('NGOS')**

5.1 It is submitted that the applicants' status as NGOs makes no material difference to the principles to be applied in determining whether the Intelligence Sharing or the s.8(4) Regime violates their rights under Art. 8 (or Art. 10) of the Convention.

5.2 The Applicants' principal challenge is to the lawfulness of the Intelligence Sharing and s.8(4) Regimes in general and, save for the issue of prior judicial authorisation which is raised in the context of Art. 10 ECHR and the s.8(4) Regime (see below), the Applicant's have not suggested that their status as Non-Governmental Organisations (NGOs) makes a material difference to the tests to be applied when considering the lawfulness of the Regimes (see the Applicants' Additional Submissions on the Facts and Complaints at §§41-73).

5.3 The Government accepts that it is possible for material emanating from NGOs to be intercepted in the course of the execution of a s.8(4) warrant. It is also possible that some of that material may be of a sensitive or privileged nature. The same applies to other categories of confidential information which may be included within 'external communications' intercepted under the s.8(4) Regime. However, in the context of a regime of strategic monitoring such as the s.8(4) Regime, which does not target NGO (or journalistic) material (whether for the purposes of identifying sources or otherwise) there is no material distinction to be drawn between NGO material and other types of material which may also be subject to untargeted interception.

5.4 In any event there are special provisions in the Code addressing the handling of confidential material as set out in detail below in the context of Art. 10 ECHR (see §§ 6.24-6.28 below)

6 ***QUESTION 4. ARTICLE 10 - THE CONVENTION PROTECTION AFFORDED TO NGOS UNDER ART. 10 ECHR***

6.1 In the light of the cases cited at §38 of *Guseva v Bulgaria*, Appl. No. 6987/07, 17 February 2015, including *Österreichische Vereinigung zur Erhaltung v. Austria*, Appl. No. 39534/07, 28 November 2013 (see in particular §§33-34), the NGOs engaged in the legitimate gathering of information of public interest in order to contribute to public debate may properly claim the same Art. 10 protections as the press. In principle, therefore, the obtaining, retention, use or disclosure of the applicants' communications and communications data may potentially amount to an interference with their Art. 10 rights, at least where the communications in question are quasi-journalistic ones, relating to their role as "social watchdogs".

The requirements of Art. 10

6.2 Although the Court has formulated a separate question addressing the merits of the applicants' case under Art. 10 of the Convention, the applicable principles are materially the same as those addressed above under Art. 8.

6.3 The only respect in which the applicants seek to contend that Art. 10 may give rise to an additional argument over and above the tests under Art. 8 is in respect of prior judicial authorisation for s. 8(4) warrants under the s.8(4) Regime (see §68 and §§78-81 of the Additional Submissions on the Facts and Complaints). That is consistent with the applicants' position during the domestic IPT proceedings where (save for the question of prior judicial authorisation under Art. 10) it was agreed between the parties that no separate argument arose in relation to Article 10(2), over and above that arising out of Article 8(2) (see the IPT's 5 December judgment at §149).

6.4 The cases to which the Court has referred in its question – *Nordisk Film*[144], *Financial Times Ltd*[145], *Telegraaf Media* and *Nagla* – are all cases concerned with targeted measures directed to the identification and/or disclosure of journalistic sources. None of them is concerned with strategic monitoring of the type conducted under the s.8(4) Regime. These cases are, therefore, to be distinguished from *Weber*,[146] and

[144] *Nordisk Film & TV A/S v Denmark* App. No. 40485/02, 8 December 2005.
[145] *Financial Times Ltd and Others v the United Kingdom*, App. No. 821/03, 15 December 2009; (2010) 50 EHRR 1153.
[146] *Weber and Saravia v Germany* (2008) 46 EHRR SE 47

the principles it identified as being applicable to a strategic monitoring regime which did not target journalistic material.

6.5 In light of the question asked by the Court, and the extent to which the applicants appear to place particular reliance on their status as NGOs (as entitling them to the same protection as journalists under Art. 10), the submissions set out below address the following three issues:

(i) Whether there is any material difference, in a case of this nature, between the principles to be applied under Article 8 and Article 10 when determining whether the measures in question are in accordance with the law/prescribed by law.

(ii) Whether the possibility that confidential journalistic (or NGO) material might be intercepted in the course of strategic monitoring under the s.8(4) Regime gives rise to considerations under Article 10 which have not been fully addressed in the analysis of Article 8 above.

(iii) Whether the particular nature of confidential journalistic (or NGO) material gives rise to a requirement for prior judicial oversight in the context of the s.8(4) regime.

The Applicable Principles

6.6 Although there is a difference in the English text of the Convention between the wording of the material provisions of Article 8 ('in accordance with the law') and Article 10 ('prescribed by law'), the Court has observed, in *Telegraaf Media*, that there is no difference in the French text which includes the formulation '*prevue(s) par la loi*' in both Articles (§89).

6.7 In §90 of *Telegraaf Media* the Court made clear that the essential requirements of Article 8(1) and Article 10(1) were the same:

> "*The Court reiterates its case-law according to which the expression "in accordance with the law" not only requires the impugned measure to have some basis in domestic law, but also refers to the quality of the law in question, requiring that it should be accessible to the person concerned and foreseeable as to its effects. The law must be*

> *compatible with the rule of law, which means that it must provide a measure of legal protection against arbitrary interference by public authorities with the rights safeguarded by Article 8 § 1 and Article 10 § 1."*

6.8 The Government therefore adopts, but does not repeat, the observations set out above as to why the s.8(4) Regime is 'in accordance with the law' for the purposes of Article 8(2).

6.9 The test of 'necessity' in a democratic society is common to both Article 8(2) and Article 10(2). The applicants do not contend that a different approach should be taken to the assessment of necessity under the two Articles. The Government therefore adopts, but does not repeat, the observations set out above as to why the s.8(4) Regime is 'necessary in a democratic society' for the purposes of Article 8(2).

Interception of Journalistic Material

6.10 The Court has drawn a sharp, and important, distinction between measures that target journalistic material, particularly for the purpose of identifying sources, and strategic monitoring of communications (and/or communications data). Thus, at §151 of *Weber*:

> *"The Court observes that in the instant case, strategic monitoring was carried out in order to prevent the offences listed in s.3 (1). It was therefore not aimed at monitoring journalists; generally the authorities would know only when examining the intercepted telecommunications, if at all, that a journalist's conversation had been monitored. Surveillance measures were, in particular, not directed at uncovering journalistic sources. The interference with freedom of expression by means of strategic monitoring cannot, therefore, be characterised as particularly serious."*

6.11 Accordingly, Article 10 adds nothing of substance to the Article 8 analysis in a case concerned with strategic monitoring. The interference with freedom of expression consequent upon such monitoring is not '*particularly serious*' and any such limited interference will be justified under Article 10(2) for the same reasons that it is justified under Article 8(2). Put differently, Article 10(2) will not require, in the case

of untargeted strategic monitoring, an enhanced level of justification in respect of confidential journalistic material beyond that which Article 8(2) will require in respect of private and/or confidential communications (and/or communications data) of different types.

6.12 The line of cases identified by the Court in its question concern a different issue, namely the application of targeted measures to individual journalists for the purposes of source identification. For obvious reasons, the Court has adopted a different approach to cases of this nature. It has repeatedly emphasised the 'potentially chilling effect' that measures which compel the identification of journalistic sources may have on the ability of the press effectively to fulfil its important 'public-watchdog' role. In light of those concerns it has set a more demanding threshold of justification for such measures.

6.13 The importance of the distinction between the 'not particularly serious' interference caused by strategic monitoring and the 'potentially chilling effect' of measures directed to source disclosure is clearly illustrated by the Court's reasoning in *Telegraaf Media*. Having determined that the 'special powers' exercised in respect of the applicants were accessible, foreseeable, and subject to sufficient safeguards, so as to be 'in accordance with the law', the Court addressed (at §95 et seq.) the applicants' contention that their status as journalists required special safeguards to ensure adequate protection of their journalistic sources.

6.14 The Court commenced its analysis of this issue by considering whether its reasoning in *Weber* was applicable. The critical feature of the measures considered in *Weber* was identified as being that they were properly to be characterised as 'strategic monitoring', for the principal purpose of identifying and averting dangers in advance. They were not targeted at journalists and they did not have the identification of journalistic sources as their aim. That being so, the interference with freedom of expression consequent upon the measures in question was not to be regarded as particularly serious, and there was no requirement for special provision for the protection of press freedom.

6.15 The Court then observed that the situation in *Telegraaf Media* was materially different to that considered in *Weber*. The difference was expressed as follows (at §97):

> *"The present case is characterised precisely by the targeted surveillance of journalists in order to determine from whence they have obtained their information. It is therefore not possible to apply the same reasoning as in Weber and Saravia."*

6.16 The distinction between strategic monitoring of the type addressed in *Weber*, and targeted measures specifically directed at the identification of journalistic sources, and the reasons for that distinction, are further explained in the Court's analysis of the second aspect of the applicants' complaint in *Telegraaf Media* namely the order to surrender documents. The potentially 'chilling effect' of such an order on press freedom was described by the Court in the following terms, at §127:

> *"Protection of journalistic sources is one of the basic conditions for press freedom, as is recognised and reflected in various international instruments including the Committee of Ministers Recommendation quoted in paragraph 61 above. Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result the vital public-watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected. Having regard to the importance of the protection of journalistic sources for press freedom in a democratic society and the potentially chilling effect an order of source disclosure has on the exercise of that freedom, such a measure cannot be compatible with Article 10 of the Convention unless it is justified by an overriding requirement in the public interest (see* Goodwin, *cited above, § 39;* Voskuil, *cited above, § 65;* Financial Times Ltd. and Others, *cited above, § 59; and* Sanoma, *cited above, § 51)."*

6.17 The potentially 'chilling effect' identified in *Telegraaf Media* derived from the act of 'source disclosure'. Similarly, in *Goodwin*[147], a case concerned with a court order requiring a journalist to surrender documents for the specific purpose of identifying one of his sources, the Court identified the potentially 'chilling effect' of such a measure as arising specifically from the order for disclosure (at §39), in contrast to

[147] *Goodwin v United Kingdom* (1996) 22 EHRR 123

some general possibility that a journalistically privileged communication might fall into the hands into the authorities in the course of a programme of strategic monitoring:

> *"Protection of journalistic sources is one of the basic conditions for press freedom, as is reflected in the laws and the professional codes of conduct in a number of Contracting States and is affirmed in several international instruments on journalistic freedoms (see, amongst others, the Resolution on Journalistic Freedoms and Human Rights, adopted at the 4th European Ministerial Conference on Mass Media Policy (Prague, 7-8 December 1994) and Resolution on the Confidentiality of Journalists' Sources by the European Parliament, 18 January 1994, Official Journal of the European Communities No. C 44/34). Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result the vital public-watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected. Having regard to the importance of the protection of journalistic sources for press freedom in a democratic society and the potentially chilling effect an order of source disclosure has on the exercise of that freedom, such a measure cannot be compatible with Article 10 (art. 10) of the Convention unless it is justified by an overriding requirement in the public interest."*[148]

6.18 In *Financial Times*, the Court, observed (at §70) that although the disclosure order in that case concerned material which 'might, upon examination' lead to source identification, and would not necessarily lead to such identification, the distinction was not a material one. The 'chilling effect' would arise '*wherever journalists are seen to assist in the identification of anonymous sources*.'

6.19 The Court returned to this issue in *Nagla*. That case concerned a search by police of a journalist's house and seizure of her date storage devices following a broadcast she had aired informing the public of an information leak from the State Revenue database. The applicant complained that she had been compelled to disclose information that had enabled a journalistic source to be identified, in violation of her right to receive and impart information as protected by Article 10. The Court held

[148] See, also *Voskuil v Netherlands* [2004] EMLR 14 465 at §65.

that the complaint fell within the sphere of protection provided by Article 10 and expressed its concern as to the potential chilling effect on press freedom in the following terms, at §82:

> *"The Court notes that the Government admitted that the search at the applicant's home had been aimed at gathering "information about the criminal offence under investigation" and that it authorised not only the seizure of the files themselves but also the seizure of "information concerning the acquisition of these files". While recognising the importance of securing evidence in criminal proceedings, the Court emphasises that a chilling effect will arise wherever journalists are seen to assist in the identification of anonymous sources (see Financial Times Ltd and Others v. the United Kingdom, no. 821/03, § 70, 15 December 2009)."*

6.20 The case of *Nordisk*, referred to by the Court in its questions, adds nothing material to this analysis. On the particular facts of *Nordisk* the material in question was regarded as consisting of the applicant's 'research material' rather than material provided by journalistic sources. The Court considered that Article 10 might be applicable in a case involving such material, observing that '*a compulsory hand over of research material may have a chilling effect on the exercise of journalistic freedom of expression*.' As with the 'journalistic source' cases addressed above, the 'chilling effect' derives from the 'handing over' of the material by the journalist to the authorities.

6.21 The Court has been clear and consistent in its identification of the potentially 'chilling effect' that may arise from the disclosure of journalistically privileged material. The potential danger arises in circumstances where the journalist is seen to assist (whether under compulsion or otherwise) in the identification of anonymous sources, and thereby infringe the duty of confidence owed by a journalist to his or her source. That is not a situation that arises in the course of the operation of the s.8(4) Regime. To the extent that journalistically privileged or NGO material may be intercepted under the s.8(4) Regime, that interception takes place without any active involvement (or 'assistance') on the part of the journalist/NGO concerned. The s.8(4) Regime does not concern 'source disclosure' of the type addressed in *Telegraaf Media*, *Nagla* and the line of earlier cases of a similar nature summarised above.

6.22 It is the potentially chilling effect on press freedom, and the ability of the press to perform its 'vital public-watchdog' role, that founds the proposition that any order for disclosure, or other measure targeted at the identification of a journalistic source, must be justified by 'an overriding requirement in the public interest.' The consistent approach of the Court in this context falls to be contrasted with the approach it has taken to non-targeted, strategic monitoring in respect of which the interference with journalistic freedom of expression is not to be regarded as 'particularly serious.'

6.23 As observed by the Court in *Weber* (at §151), in the context of a regime of strategic monitoring, which is not targeted to the communications of journalists (or any other group) it will only be when an intercepted communication is selected for examination that it will (or may) become apparent that the communication contains journalistic material. The Code contains a number of specific safeguards directed to preserving the confidentiality of journalistic material in such circumstances.

6.24 In fact, and notwithstanding the submissions set out above, the s.8(4) Regime does include special provisions in respect of journalistic and confidential information. At §4.2 of the Code it states:

> "*Particular consideration should also be given in cases where the subject of the interception might reasonably assume a high degree of privacy, or where confidential information is involved. This includes where the communications relate to legally privileged material; where confidential journalistic material may be involved; where interception might involve communications between a medical professional or Minister of Religion and an individual relating to the latter's health or spiritual welfare; or where communications between a Member of Parliament and another person on constituency business may be involved.*"[149]

As is evident from the first sentence above, the requirement for "particular consideration" applies to any material where the subject of the interception might assume a high degree of privacy or where confidential information is involved and the Code does not provide an exhaustive definition of when material will fall into that category.

[149] And similar provisions were to be found in the 2002 Code see §§3.2-3.11.

6.25 In addition the definition of "confidential journalistic material" is a broad one under the Code. At §4.3 it states:

> *"Confidential journalistic material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking..."*

6.26 At §4.32, the Code states that the safeguards set out in § 4.28-4.31 are to be applied to any s.8(4) material which is selected for examination and which constitutes confidential information (including confidential journalistic material). The material elements of Code requiring as follows:

> *"4.29. Material which has been identified as confidential information should be retained only where it is necessary and proportionate to do so for one or more of the authorised purposes set out in section 15(4). It must be securely destroyed when its retention is no longer needed for those purposes. If such information is retained, there must be adequate information management systems in place to ensure that continued retention remains necessary and proportionate for the authorised statutory purposes.*
> *4.30. Where confidential information is retained or disseminated to an outside body, reasonable steps should be taken to mark the information as confidential. Where there is any doubt as to the lawfulness of the proposed handling or dissemination of confidential information, advice should be sought from a legal adviser within the relevant intercepting agency and before any further dissemination of the material takes place.*
> *4.31. Any case where confidential information is retained should be notified to the Interception of Communications Commissioner as soon as reasonably practicable, as agreed with the Commissioner. Any material which has been retained should be made available to the Commissioner on request."*

6.27 Although the applicants do not appear to raise any separate, specific complaint as regards the Intelligence Sharing Regime and NGO confidence, it is to be noted that in Chapter 12 of the Code it makes clear that such material is to be handled in the same

way as material which is obtained directly by the Intelligence Agencies (see §12.6[150]) i.e. the same safeguards as set out above would apply to confidential material including confidential journalistic material obtained pursuant to the Intelligence Sharing Regime (see §6.26).

6.28 Accordingly there are detailed provisions of the Code which provide special protection for confidential material including confidential journalistic material.

6.29 To this extent, the safeguards under the s.8(4) Regime are more rigorous than those considered to be sufficient by the Court in *Weber*. At §151, the Court noted that there were no 'special rules' forming part of the regime under the G10 Act as to how journalistic material should be treated in the event that such material was selected for examination. However, it did not regard such rules as necessary in light of the general safeguards forming part of the scheme as a whole:

> *"It is true that the impugned provisions of the amended G10 Act did not contain special rules safeguarding the protection of freedom of the press and, in particular, the non-disclosure of sources, once the authorities had become aware that they had intercepted a journalist's conversation. However, the Court, having regard to its findings under Art.8 , observes that the impugned provisions contained numerous safeguards to keep the interference with the secrecy of telecommunications – and therefore with the freedom of the press – within the limits of what was necessary to achieve the legitimate aims pursued. In particular, the safeguards which ensured that data obtained were used only to prevent certain serious criminal offences must also be considered adequate and effective for keeping the disclosure of journalistic sources to an unavoidable minimum. In these circumstances the Court concludes that the respondent State adduced relevant and sufficient reasons to justify interference with freedom of expression as a result of the impugned provisions by reference to the legitimate interests of national security and the prevention of crime. Having regard*

[150] Which provides, as follows: "*Where intercepted communications content or communications data are obtained by the intercepting agencies as set out in paragraph 12.2, or are otherwise received by them from the government of a country or territory outside the UK in circumstances where the material identifies itself as the product of an interception, (except in accordance with an international mutual assistance agreement), the communications content… and communications data… must be subject to the same internal rules and safeguards that apply to the same categories of content or data when they are obtained directly by the intercepting agencies as a result of interception under RIPA.*"

to its margin of appreciation, the respondent State was entitled to consider these requirements to override the right to freedom of expression."

6.30 Whilst the specific safeguards set out in the Code in relation to confidential material may not be necessary to ensure compliance with Articles 8 and/or 10 in the context the s.8(4) Regime of strategic monitoring, the fact that such safeguards exist is clearly sufficient to address any assertion by the applicants that specific safeguards are required in respect of NGO material where the applicants are in communication with sources (see §78 of the applicants' Additional Submissions on the Facts and Complaints).

Prior Judicial Authorisation

6.31 As already noted, the Court's case law does not require independent authorisation of warrants as a precondition of the lawfulness of interception of communications (or communications data), provided that the applicable regime otherwise contains sufficient safeguards: see §§4.96-4.97 above.

6.32 Nor has the Court established a rule requiring prior judicial authorisation for state interference with journalistic freedom. In some cases prior judicial scrutiny has been found to be necessary, in others it has not.

6.33 In *Sanoma Uitgevers BV v The Netherlands*[151], the Court was concerned with a Dutch law authorising the compulsory surrender of material to the police for use in a criminal investigation. It was, therefore, a case concerned with targeted measures to compel disclosure of journalistic sources (such as *Goodwin, Financial Times*, and *Telegraaf Media*) rather than a regime of strategic monitoring in the course of which journalistic material might be intercepted (*Weber*). It was in this context that the Court identified the importance of prior authorisation by a Judge or other independent body:

"89. The court notes that orders to disclose sources potentially have a detrimental impact, not only on the source, whose identity may be revealed, but also on the

[151] [2011] EMLR 4

newspaper or other publication against which the order is directed, whose reputation may be negatively affected in the eyes of future potential sources by the disclosure, and on members of the public, who have an interest in receiving information imparted through anonymous sources …

92. Given the preventive nature of such review the judge or other independent and impartial body must thus be in a position to carry out this weighing of the potential risks and respective interests prior to any disclosure and with reference to the material that it is sought to have disclosed so that the arguments of the authorities seeking the disclosure can be properly assessed."

6.34 Similarly, in *Telegraaf Media*, another case concerned with the targeted measures directed against journalists with a view to obtaining knowledge of their sources, the Court considered that a post factum review was insufficient in circumstances where, once the confidentiality of journalistic sources had been destroyed, it could not be repaired. The Court's conclusion was expressly tied to the nature and purpose of the powers being exercised, (at §102):

"The court thus finds that the law did not provide safeguards appropriate to the use of powers of surveillance against journalists with a view to discovering their journalistic sources. There has therefore been a violation of articles 8 and 10 of the Convention.

6.35 The Court of Appeal in *Miranda*[152] considered the judgment of the Court in *Nagla*, and decided that it supported the proposition that a requirement for prior judicial authorisation could extend beyond cases involving source disclosure to cases concerned with the seizure of a journalist's material, such as computers, hard drives and memory cards. It was observed (at §113) that such seizure of journalistic material, even if not directly concerned with the identification of a source, could serve to create a 'chilling effect' of a similar nature to that created by measures expressly directed to source identification.

6.36 The extent to which an order permitting the seizure of journalistic material, for purposes other than source identification, will have a chilling effect on the freedom

[152] *R (Miranda) v Secretary of State for the Home Department* [2016] EWCA Civ 6 (See Annex 54).

of journalistic expression is likely to depend on the facts of the case and the Court has adopted a carefully fact-sensitive approach to cases of this nature. However, there is clearly a material difference between an order specifically directed to the seizure of (for example) a journalist's computer and the operation of a strategic monitoring regime under which a journalist's communications (or communications data) may be intercepted in the course of a large-scale and untargeted programme of interception.

6.37 There is no authority in the Court's caselaw[153] for the proposition that prior judicial (or independent) authorisation is required for the operation of a strategic monitoring regime such as the s.8(4) Regime, by virtue of the fact that some journalistic (or NGO) material may be intercepted in the course of that regime's operation. The only circumstances in which such a requirement has been found to exist is in respect of targeted measures directed at the identification of journalistic sources and/or the seizure of journalist's material.

6.38 Even if it were considered desirable in principle, a requirement of prior judicial authorisation in the operation of the s.8(4) Regime would be of no practical effect, as observed by the IPT in the Liberty proceedings in the 5 December judgment, at §151:

> *"We are in any event entirely persuaded that this, which is not of course a case of targeted surveillance of journalists, or indeed of NGOs, is not such an appropriate case, particularly where we have decided in paragraph 116(vi) above, that the present system is adequate in accordance with Convention jurisprudence without prior judicial authorisation. In the context of the untargeted monitoring by s.8 (4) warrant, it is clearly impossible to anticipate a judicial pre-authorisation prior to the warrant limited to what might turn out to impact upon Article 10. The only situation in which it might arise would be in the event that in the course of examination of the contents, some question of journalistic confidence might arise. There is, however, express provision in the Code (at paragraph 3.11), to which we have already referred, in relation to treatment of such material."*

[153] Or the domestic case law for that matter.

6.39 Those observations are clearly correct. A requirement of prior judicial authorisation in respect of journalistic or NGO material under a regime of strategic (non-targeted) monitoring such as the s.8(4) Regime would simply make no sense. All that a Judge could be told is that there was a possibility that the execution of the warrant might result in the interception of some confidential journalistic/NGO material (along with other categories of confidential material). In the event that any such material was selected for examination the relevant provisions of the Code would apply.

7 QUESTION 5: ARTICLE 6 OF THE CONVENTION

The rights at issue are not "civil rights".

7.1 In *Klass*, the Commission (Report of the Commission, Series B, no. 26 pp35-37) concluded that the applicants' right to protection of secrecy for correspondence and telecommunications was not a "civil" right for the purposes of Art. 6(1). In particular, it held at §58:

> *"...to determine what is the scope meant by 'civil rights' in Art. 6, some account must be take of the legal tradition of the Member-States. Supervisory measures of the kind in question are typical acts of State authority in the public interest and are carried out jure imperii. They cannot be questioned before any court in many legal systems. They do not at all directly concern private rights. The Commission concludes therefore, that Art. 6 does not apply to this kind of State interference on security grounds."*

7.2 The Court approved this conclusion in *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* app. 62540/00, 28 June 2007, at §106; a case which concerned the compatibility of Bulgarian legislation allowing the use of secret surveillance measures with Articles 6, 8 and 13 ECHR. Consequently it is clear that Art. 6 did not apply to the domestic IPT proceedings[154].

[154] It is to the noted that the IPT's own conclusion to the contrary in its Preliminary Issues Ruling in *Kennedy* (IPT/01/62) dated 9 December 2004, at §§85-108 was issued before the Court's judgment in *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* .

7.3 That conclusion is also consistent with the Court's reasoning in *Klass* in relation to the issue of judicial control of interception powers – see §§57-58[155]. Since the Convention must be read as a whole, the applicants' Art. 6 complaints in *Klass* had to be addressed in a manner that was consistent with the Court's conclusion on the appropriateness of judicial control under Art. 8. Accordingly, as regards Article 6 the Court held at §75:

> *"The Court has held that in the circumstances of the present case the G 10 does not contravene Article 8 in authorising a secret surveillance of mail, post and telecommunications subject to the conditions specified...*
>
> *Since the Court has arrived at this conclusion, the question whether the decisions authorising such surveillance under the G 10 are covered by the judicial guarantee set forth in Article 6 – assuming this Article to be applicable – must be examined by drawing a distinction between two stages: that before, and that after, notification of the termination of surveillance.*
>
> *As long as it remains validly secret, the decision placing someone under surveillance is thereby incapable of judicial control on the initiative of the person concerned,*

[155] Where the Court stated:

> *"... it is necessary to determine whether judicial control, in particular with the individual's participation, should continue to be excluded even after surveillance has ceased. Inextricably linked to this issue is the question of subsequent notification, since there is in principle little scope for recourse to the courts by the individual concerned unless he is advised of the measures taken without his knowledge and thus able retrospectively to challenge their legality. In the opinion of the Court, it has to be ascertained whether it is even feasible in practice to require subsequent notification in all cases.*
>
> *The activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures. Subsequent notification to each individual affected by a suspended measure might well jeopardise the long-term purpose that originally prompted the surveillance. Furthermore, as the Federal Constitutional Court rightly observed, such notification might serve to reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents. In the Court's view, in so far as the 'interference' resulting from the contested legislation is in principle justified under Article 8 (2) (see para. 48 above), the fact of not informing the individual once surveillance has ceased cannot itself be incompatible with this provision, since it is this very fact which ensures the efficacy of the 'interference'. Moreover, it is to be recalled that, in pursuance of the Federal Constitutional Court's judgment of 15 December 1970, the person concerned must be informed after the termination of the surveillance measures as soon as notification can be made without jeopardising the purpose of the restriction..."*

> *within the meaning of Article 6; as a consequence, it of necessity escapes the requirements of that Article.*
>
> *The decision can come within the ambit of the said provision only after discontinuance of the surveillance. According to the information supplied by the Government, the individual concerned, once he has been notified of such discontinuance, has at his disposal several legal remedies against the possible infringements of his rights; these remedies would satisfy the requirements of Article 6 ...*
>
> *The Court accordingly concludes that, even if it is applicable, Article 6 has not been violated."*

7.4 The Court's judgment in *Klass* thus establishes that the requirements of Art. 6 cannot apply to a dispute concerning the interception powers insofar as the use of such powers in the case at issue remains validly secret (see the highlighted words in the passage above)[156].

7.5 The applicants' case clearly falls within the scope of this finding. During the domestic IPT proceedings the applicants' case was that there was a continuing situation of intelligence sharing/interception; it was not contended that there had been such interferences in the past and that the applicants could now be safely notified of that fact. Consequently at the time of the IPT proceedings, the Government adopted a stance of "neither confirm nor deny" (see §4(ii) of the 5 December judgment) and the legal issues were determined on the basis of hypothetical facts. Applying *Klass*, this was not a situation where Art. 6 applied.

7.6 The Court's conclusion in *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* that the rights at issue in the field of secret interception powers are not "civil" rights is further supported by the Court's more general jurisprudence on the meaning of "civil rights and obligations".

[156] The Court's approach to Art. 6 in *Klass* is consistent with the approach to Art. 13 in the context of secret surveillance powers – see eg. *Leander v Sweden* at §77(d).

7.7 As the Grand Chamber confirmed at §28 of *Ferrazzini v Italy* app. 44759/98, 12 July 2001, the mere fact that an individual enjoys rights or owes obligations does not in itself mean that those rights and obligations are "civil" for the purposes of Art. 6. The text of Art. 6 cannot be interpreted as if the adjective "civil" were not present (*Ferrazzini* at §30). It is clear that secret powers of intelligence gathering/interception that are used solely in the interests of national security or to detect serious crime, form part of the "*hard core of public-authority prerogatives*" so as to render it inappropriate to classify any related rights and obligations as "civil" in nature – see *Ferrazzini* at §§27-29[157] (and see also the reference to "discretionary powers intrinsic to state sovereignty" at §61 of *Vilho Eskelinen v Finland*, app. 63235/00, 19 April 2007).

7.8 Further, merely showing (or simply asserting) that a dispute is "pecuniary" in nature is not, in itself, sufficient to attract the applicability of Art. 6(1) under its "civil" head, see §25 of *Ferrazzini*. It follows, *a fortiori*, that the mere fact that in the IPT proceedings the Applicants' claimed, among other remedies, financial compensation, does not mean that Art. 6 is applicable to those IPT proceedings. Similarly, as the

---

[157] Where the Court stated, *inter alia*:

> "*27. Relations between the individual and the State have clearly evolved in many spheres during the fifty years which have elapsed since the Convention was adopted, with State regulation increasingly intervening in private-law relations. This has led the Court to find that procedures classified under national law as being part of "public law" could come within the purview of Article 6 under its "civil" head if the outcome was decisive for private rights and obligations, in regard to such matters as, to give some examples, the sale of land, the running of a private clinic, property interests, the granting of administrative authorisations relating to the conditions of professional practice or of a licence to serve alcoholic beverages...*
>
> *28. However, rights and obligations existing for an individual are not necessarily civil in nature. Thus, political rights and obligations, such as the right to stand for election to the National Assembly (see Pierre-Bloch, cited above, p. 223, § 50), even though in those proceedings the applicant's pecuniary interests were at stake (ibid., § 51), are not civil in nature, with the consequence that Article 6 § 1 does not apply…. Similarly, the expulsion of aliens does not give rise to disputes (contestations) over civil rights for the purposes of Article 6 § 1 of the Convention, which accordingly does not apply (see Maaouia, cited above, §§ 37-38).*
>
> *29. In the tax field, developments which might have occurred in democratic societies do not, however, affect the fundamental nature of the obligation on individuals or companies to pay tax. In comparison with the position when the Convention was adopted, those developments have not entailed a further intervention by the State into the "civil" sphere of the individual's life. The Court considers that tax matters still form part of the hard core of public-authority prerogatives, with the public nature of the relationship between the taxpayer and the community remaining predominant…*"

Grand Chamber confirmed at §38 of *Maaouia v France*, app. 39652/98, 5 October 2000, the fact that a dispute may have major repercussions on an individual's private life does not suffice to bring proceedings within the scope of "civil" rights protected by Art. 6(1).

7.9 Finally, the fact that the Applicants had the right, as a matter of domestic law, to complain to the IPT does not make the rights at issue "civil". As recognised by the Grand Chamber in *Ferrazzini* at §24, the concept of "civil rights and obligations" is "autonomous" within the meaning of Art. 6(1) and thus it cannot be interpreted solely by reference to the domestic law of the respondent State. In addition the Tribunal is specifically designed to operate under the constraints recognised by the Court at §57 of *Klass* (and upon which the Court's conclusion in *Klass* under Art. 6 was based). In particular, a complainant in the Tribunal is not permitted to participate in any factual inquiry that the Tribunal may conduct into the allegations that he has made: eg. the fact of any interception remains secret throughout (save, of course, where the Tribunal finds unlawfulness to have occurred). Thus the fact that RIPA offers individuals the additional safeguard (under Art. 8) of an unlimited right to complain to the Tribunal cannot in itself make Art. 6 apply to such disputes.

If the proceedings did involve the determination of "civil, rights", were the restrictions in the IPT proceedings, taken as a whole, disproportionate or did they impair the very essence of the applicants' right to a fair trial? (see Kennedy v the United Kingdom, no 26839/05, §186, 18 May 2010)

7.10 In the alternative, even if Art. 6 did apply to the proceedings before the IPT, it was satisfied. The IPT's procedures, which must take account of the legitimate need, based in national security, for the protection so sensitive information, plainly did not impair the very essence of the applicants' right to a fair trial, particularly given the Court's conclusions in the *Kennedy* case.

(1) Article 6 - the core principles

Disclosure rights not absolute

7.11 It is well established that although the right to a fair process is unqualified, the constituent elements or requirements of a fair process are not absolute or fixed: see *Brown v Stott* [2003] 1 AC 681 at 693D-E per Lord Bingham (See Annex 60); 719G-H per Lord Hope; 727H per Lord Clyde. In *Brown v Stott*, Lord Bingham stated at 704D:

> "*The jurisprudence of the European court very clearly establishes that while the overall fairness of a criminal trial cannot be compromised, the constituent rights comprised, whether expressly or implicitly, within article 6 are not themselves absolute.*"

7.12 The approach of the Court in considering issues of fairness is therefore context and fact sensitive. This was re-affirmed by the Court in *A & Others v United Kingdom*, no. 3455/05, §203, 19 February 2009, when considering the requirements of Article 5(4). The Court stated in terms:

> "*The requirement of procedural fairness under Article 5(4) does not impose a uniform unvarying standard to be applied irrespective of the context, facts and circumstances.*"

a. The context specific nature of the analysis of the requisite ingredients of fairness was emphasised at §217. The Court specifically tied its conclusions as to the ingredients of fairness to the particular context of that case:

> "*in the circumstances of the present case, and in view of the dramatic impact of the lengthy – and what appeared at that time to be indefinite – deprivation of liberty on the applicants' fundamental rights, Article 5(4) must import substantially the same fair trial guarantees as Article 6(1) in its criminal aspect.*"
>
> Further at §220 the Court reinforced that each case must be considered on a "case-by-case basis", in line with its conclusion at §203.

7.13 This approach of the Court has been acknowledged by the domestic courts. In *R v H* [2004] 2 AC 134 (See Annex 61), Lord Bingham noted at §33:

> "*The consistent practice of the Court, in this and other fields, has been to declare principles, and apply those principles on a case-by-case basis according to the particular facts of the case before it, but to avoid laying down rigid or inflexible rules. … It is entirely contrary to the trend of Strasbourg decision-making to hold that in a certain class of case or when a certain kind of decision has to be made a prescribed procedure must always be followed.*"

7.14 The approach of the Court also acknowledges that the necessary ingredients of fairness can, and should, take into account what is at stake both for the individual concerned and for the general community. Consistently with this approach, the Court has recognised that the ingredients of fairness in the civil context may be different to i.e. lighter than and more flexible than those that apply in the criminal context: *Dombo Beheer v The Netherlands*, no. 14448/88, §32, 27 October 1993. That is also recognised in the structure and content of Article 6 itself: see Articles 6(2) and (3) ECHR. As stated in *Vanjak v Croatia*[158] at §45:

> "*The requirements inherent in the concept of fair hearing are not necessarily the same in cases concerning the determination of civil rights and obligations as they are in cases concerning the determination of a criminal charge. This is borne out by the absence of detailed provisions such as paragraphs 2 and 3 of Article 6 applying to cases of the former category. Thus, although these provisions have a certain relevance outside the strict confines of criminal law (see, mutatis mutandis, Albert and Le Compte v. Belgium, 10 February 1983, Series A no. 58, § 39), the Contracting States have greater latitude when dealing with civil cases concerning civil rights and obligations than they have when dealing with criminal cases (see Pitkänen v. Finland, no. 30508/96, § 59, 9 March 2004).*"

7.15 Accordingly, very considerable caution is needed before concluding that an ingredient considered necessary in a context at one end of the spectrum (eg. a criminal case or a case involving deprivation or severe restriction of liberty) is also necessary in a context at the other end of the spectrum (eg. a complaint of unlawful interception in breach of qualified rights under the Convention).

---

[158] Application no. 29889/04 dated 14 January 2010

7.16 As to **disclosure**, in *Rowe and Davis v United Kingdom*, no. 28901/95, 16 February 2000 a criminal case, the Court stated at [60]:

> "*It is a fundamental aspect of the right to a fair trial that criminal proceedings, including the elements of such proceedings which relate to procedure, should be adversarial and that there should be equality of arms between the prosecution and defence. The right to an adversarial trial means, in a criminal case, that both prosecution and defence must be given the opportunity to have knowledge of and comment on the observations filed and the evidence adduced by the other party. In addition, Article 6(1) requires, as indeed does English law, that the prosecution authorities should disclose to the defence all material evidence in their possession for or against the accused.*"

7.17 Whilst the general right to disclosure of the case against the individual and of the relevant evidence is clearly established "in a criminal case", even in that context the general right is not absolute. It is not one of the express procedural rights set out in Art. 6. The general right is implied into Article 6 as an aspect of the express right to a fair trial. Implied rights are in principle subject to necessary and proportionate restrictions.

7.18 It follows that the Court has held that the right to disclosure can be limited by reference to the rights and interests of others and the public interest and that is so even in the context of criminal proceedings. For example:

(1) In *Doorson v The Netherlands* (1996), no. 20524/92, §70, 26 March 1996 and *Van Mechelen v The Netherlands*, no. 21363/93; 21364/93; 21427/93;22056/93, §52-54, 23 April 1997 the ECtHR held that the principles of fair trial require that in appropriate cases the interests of the defence are balanced against those of witnesses or victims, and therefore that the use of statements made by anonymous witnesses to found a criminal conviction was not in principle incompatible with Art. 6.

(2) In *Jasper v United Kingdom*, no. 27052/95, §52, 16 February 2000 the ECtHR held that limitations on disclosure of relevant evidence could in principle be justified

on public interest immunity grounds in order to keep secret police methods of investigation of crime.

(3) In *Tinnelly & Sons Ltd and McElduff v United Kingdom, no. 20390/92; 21322/92,* §71-78, *10 July 1998* and *A v United Kingdom* at §§205-206, the ECtHR held that restrictions on the right to a fully adversarial procedure may in principle be permissible where strictly necessary to protect national security.

7.19 These limitations reflect the fact that there is a balance inherent in the whole of the Convention between the rights of the individual and the rights and interests of the community as a whole: see, eg, *Soering v United Kingdom*, no. 14038/88, §89, 19 January 1989.

7.20 That balance recognises that other rights and other vital interests may be in play. National security, which is not an end in itself but a necessary component in the protection of the public from serious threats and harm, is one important example. The Court has long recognised that the need to protect a State's citizens from risk of terrorist attack is one of the most pressing competing interests: see, for example, *Klass v Germany*, no. 5029/71, §48, 6 September 1978 and *Chahal v United Kingdom, no. 22414/93,* §79, 15 November 1996.

7.21 Thus, so far as civil proceedings are concerned, there is scope under the Convention for restrictions on the general position of full disclosure of relevant material when determining civil rights and obligations.

Principles governing permissible limitations on implied rights

7.22 It is of course acknowledged that the usual position is that fairness, even in civil proceedings, requires full disclosure of all information relevant to the issues being determined; and requires a reasoned judgment referring as necessary to all such relevant information. However, it is equally clear that that approach can be subject to limitations. Specifically national security considerations can, and in some circumstances must, impact on the specific ingredients of fairness. In practice such considerations will render it difficult, and on occasion impossible, to open up information relevant to the issues.

7.23 When assessing whether a particular limitation is permissible under Article 6, the approach of the Court has been constant. It asks two questions:

(1) Is the restriction "strictly necessary"? It must be directed to a proper social objective and go no further than is required to meet that objective; and

(2) Is the restriction "sufficiently counterbalanced" by the procedures in place?

(See *Tinnelly & Sons Ltd v United Kingdom*, no. 20390/92; 21322/92, §72, 10 July 1998 *Rowe and Davis v United Kingdom* at §61; *Botmeh and Alami v United Kingdom*, no. 15187/03, §37, 7 June 2007 *Kennedy v United Kingdom* at §180).

7.24 As to necessity, there is a clear and consistent line of Court jurisprudence recognising that the protection of national security interests (which exist in order to protect the rights and interests of the public, including in particular their safety) provides a legitimate basis on which material may have to be withheld: see eg *Leander v Sweden*, no. 9248/81, §49, §59 and §66, 26 March 1987, *Tinnelly & Sons v United Kingdom* at §76; *A v United Kingdom* at §§205-206 and §218 and *Kennedy v UK* at §§184-190.

7.25 In addition the Court has emphasised that the primary procedural safeguard is the scrutiny which can be provided by an independent court, fully appraised of all relevant material (see *Tinnelly & Sons Ltd & McElduff v United Kingdom* at §78 and see *Liu & Liu v Russia*, no. 29157/09, 26 July 2011 at §61 and §63[159]).

Kennedy v United Kingdom

7.26 In *Kennedy* the Court considered that scrutiny of relevant material by the IPT provided sufficient procedural safeguards against abuse.

[159] See also the similar cases of *Dağtekin v Turkey* (App. No. 70516/01) (13 December 2007) and *Gencer v Turkey* (App. No. 31881/02) (25 November 2008), both of which concerned the annulment on national security grounds of the applicants' right to farm land (which deprived them of their livelihoods). In those cases, the Court concluded that the applicants were deprived of sufficient procedural safeguards because the conclusions of the security investigation were not communicated to the domestic courts.

7.27 The Court noted the extensive jurisdiction of the IPT to examine any complaint of unlawful interception which included: the independence and impartiality of the IPT and the judicial experience of its members; the fact that the IPT had access to closed material and the power to order disclosure of relevant documents by those involved in the authorisation and execution of a warrant; and that the IPT's legal rulings were published: §167.

7.28 The Court held that the need to keep secret sensitive and confidential information justified the strong restrictions on disclosure of relevant information in proceedings before the IPT in the UK. Almost all of the relevant information considered and relied upon by the IPT was not disclosed to the applicant. The needs of national security precluded such a course. The Court assumed (without deciding) that Article 6(1) was engaged. Yet, the Court held that the IPT's procedures complied with the fairness requirement in Art. 6.

7.29 Critically, the Court found that the need to retain the secrecy of any surveillance measures was decisive in determining the extent of procedural safeguards, stating at §§186-187:

> "*At the outset, the Court emphasises that the proceedings related to secret surveillance measures and that there was therefore a need to keep secret sensitive and confidential information. In the Court's view, this consideration justifies restrictions in the IPT proceedings. The question is whether the restrictions, taken as a whole, were disproportionate or impaired the very essence of the applicant's right to a fair trial.*
>
> > *In respect of the rules limiting disclosure, the Court recalls that the entitlement to disclosure of relevant evidence is not an absolute right. The interests of national security or the need to keep secret methods of investigation of crime must be weighed against the general right to adversarial proceedings. … The Court further observes that documents submitted to the IPT in respect of a specific complaint, as well as details of any witnesses who have provided evidence, are likely to be highly sensitive, particularly when viewed in light of the Government's 'neither confirm nor*

> *deny' policy. The Court agrees with the Government that, in the circumstances, it was not possible to disclose redacted documents or to appoint special advocates as these measures would not have achieved the aim of preserving the secrecy of whether any interception had taken place."*

7.30 Accordingly, the ECtHR concluded at §190 that:

> *"...the restrictions on the procedure before the IPT did not violate the applicant's right to a fair trial. In reaching this conclusion the Court emphasises the breadth of access to the IPT enjoyed by those complaining about interception within the United Kingdom and the absence of any evidential burden to be overcome in order to lodge an application with the IPT. In order to ensure the efficacy of the secret surveillance regime, and bearing in mind the importance of such measures to the fight against terrorism and serious crime the Court considers that the restrictions on the applicant's rights in the context of the proceedings before the IPT were both necessary and proportionate and did not impair the very essence of the applicant's Article 6 rights."*

7.31 Consequently, despite the paucity of disclosure in open in that case, the Tribunal proceedings were nevertheless Art. 6(1) compliant.

The appointment of Counsel to the Tribunal (CTT)

7.32 In *Kennedy* the Court agreed with the Government that, in the circumstances of that case, it was not possible to appoint special advocates, as such a step could not have achieved the aim of preserving the secrecy of whether any interception had taken place (see §187).

7.33 However in the Liberty IPT proceedings (which involved general challenges to the regimes governing the intelligence sharing and s.8(4) regimes), CTT were appointed and, in practice, they performed an essentially similar function to special advocates (see §10 of the 5 December judgment). That included reviewing the CLOSED disclosure provided to the Tribunal to identify documents, parts of documents or gists that ought properly to be disclosed and making submissions to the IPT in

favour of disclosure as were in the interests of the claimants and open justice (see §10 of the 5 December judgment).

7.34 In a series of cases the Court has emphasised the role which can be played by special advocates as a safeguard where closed procedures are deployed: see *Chahal v United Kingdom*. no. 22414/93, 15 November 1996, at §144, *Jasper v United Kingdom* at §§36-38 and §55, *Al-Nashif v Bulgaria,* app. 50963/99, §§95-97, 20 June 2002, *A & others v United Kingdom at* §220 and *Othman (Abu Qatada) v United Kingdom*[160] at §§222-224. In *Othman* the Court emphasised the "rigorous scrutiny" which can be provided by special advocates, particularly where there are issues of a general nature which do not depend upon specific instructions from an individual claimant (see, in particular, §§223-224).

7.35 Consequently, the appointment of CTT in the IPT proceedings (acting effectively as special advocates) is a further important counterbalance to any compromise in the fairness of the proceedings due to the requirements of national security. As was the position in *Othman,* CTT can be particularly effective in IPT proceedings where the issues in the case do not require specific instructions from individuals (eg. about a positive national security case against them) and where eg. the central issue is the compatibility of the regime with ECHR standards. CTT is well-placed to make submissions in CLOSED to the IPT on the CLOSED disclosure provided to the IPT and its significance in terms of the lawfulness of the regimes.

Fairness of the IPT proceedings in Liberty

7.36 The Applicants have made a number of specific criticisms about the fairness of the IPT proceedings, each of which has been considered in turn below. Overall it is submitted that the IPT proceedings were patently fair given the following particular features of the proceedings:

(1) The applicants did not have to overcome any evidential burden to apply to the IPT.

(2) There was scrutiny of <u>all</u> the relevant material, open and closed, by the

[160] Application No. 8139/09 17 January 2012, 32 B.H.R.C. 62

IPT, which had full powers to obtain any material it considered necessary.

(3) Material was only withheld in circumstances where the IPT was satisfied that there were appropriate public interest and national security concerns.

(4) The Tribunal appointed Counsel to the Tribunal (CTT) who, in practice, performed a similar function to that performed by a Special Advocate in closed material proceedings. CTT was well placed to represent the interests of the applicants in closed hearings given the issues which the IPT was considering (which did not turn on specific instructions from the applicants themselves).

7.37 As to the specific complaints raised by the Applicants, **first** it is said that the IPT declined to direct the intelligence services to disclose any of their internal guidance concerning the treatment of confidential material of non-government organisations (NGOs) under Art. 10. This is addressed at §§134-135 of the IPT's 5 December judgment. As is evident from that extract from the judgment:

(1) Liberty only sought to raise, at a very late stage of the IPT proceedings (in written submissions dated 17 November 2014), the issue whether there was adequate provision under Art. 10 ECHR for dealing with confidential information in the context of NGO activities ('NGO confidence');

(2) The issue of NGO confidence was not raised when the legal issues were agreed between all parties on 14 February 2014, some 5 months before the open legal issues hearing in July 2014;

(3) The written arguments addressed at the July 2014 hearing had not raised any separate issue under Art. 10 ECHR in respect of NGO confidence.

(4) Liberty had been given ample opportunity to raise the issue, but had not done so.

(5) The IPT concluded that it was far too late (in November 2014) to be seeking to raise the issue, particularly in circumstances where it was being suggested that further disclosure and "considerable" further argument would be necessary to incorporate it into the proceedings at that stage.

7.38 In those circumstances, the IPT cannot be criticised for declining to address this additional issue at the hearing and thereby not pursuing any separate issue of disclosure which arose in relation to it.

7.39 **Secondly**, the Applicants state that the IPT took the position that it had no power, in any event, to require the intelligence services to disclose such evidence. But there is no finding in the IPT's judgments to the effect that it had no power to require the intelligence services to disclose such evidence. That was not a live issue in the proceedings, in circumstances where the Intelligence Agencies had agreed to make all of the disclosure which the IPT had suggested. As stated at §10 if the IPT judgment dated 5 December:

> *"...As will be seen, in the context of a closed hearing there were matters derived from the evidence in the closed hearing which the Respondents were prepared to consent to disclose, and there were no matters which the Tribunal considered should be disclosed which the Respondents declined to disclose. Written submissions by the parties and a further closed and open hearing then followed, and some further matters were disclosed voluntarily by the Respondents."*(emphasis added)

7.40 It is therefore wrong to suggest that the IPT took the position that it had no power to order disclosure in the proceedings; that issue did not arise in the proceedings given that the Respondents were content to disclose that which the Tribunal suggested should be disclosed.

7.41 **Thirdly** the applicants assert that the IPT wrongly held a closed hearing on whether the relevant framework governing the intelligence services' interception and receipt of material of foreign intelligence agencies was in accordance with the law. But there was no breach of Art. 6 in that approach. As explained by the IPT, the matters which were considered in closed were too sensitive for discussion in open court for reasons of national security and the public interest. In addition, part of the purpose of considering the agencies' internal arrangements in closed was to consider their adequacy and whether any of them could be publicly disclosed – see §7 and 46(iii)-(iv) of the 5 December judgment:

"After the five day public hearing, we held a one day closed hearing to consider certain matters which were, in the considered judgment of the Respondents, too confidential and sensitive for discussion in open court in the interests of preserving national security, and in accordance with our jurisdiction to hold such a closed hearing pursuant to Rule 9 of the Investigatory Powers Tribunal Rules 2000. As will appear, we considered in particular the arrangements,...described during the public hearing as "below the waterline", regulating the conduct and practice of the Intelligence Services, in order to consider (i) their adequacy and (ii) whether any of them could and should be publicly disclosed in order to comply with the requirements of Articles 8 and 10 of the Convention as interpreted by the ECtHR, to which we will refer further below.

...[The IPT] has access to all secret information, and can adjourn into closed hearing in order to assess whether the arrangements (a) do indeed exist as asserted by Mr Farr, (b) are adequate to do the job of giving the individual "adequate protection against arbitrary interference.

[The IPT] has, and takes, the opportunity, with the benefit of full argument, to probe fully whether matters disclosed to it in closed hearing, pursuant to the Respondents' obligation to do so pursuant to s.68(6) of RIPA, can and should be disclosed in open and thereby publicised."

7.42 Consequently the IPT's approach of considering the internal arrangements in closed enabled the IPT to consider whether more could be said about them in open and, in fact, further disclosures were made in respect of such arrangements, as is evident from §10, §46, §47 and §126 of the 5 December judgment.

7.43 In addition CTT were appointed in the proceedings and made submissions from the perspective of the claimants in the closed hearing, both on the issue of disclosure and in order to ensure that all relevant arguments on the facts and the law were put to the tribunal. CTT summarised their functions in terms which largely accorded with

the claimants' submissions on what those functions should be[161]; and the IPT specifically adopted that summary[162]. The summary stated, *inter alia*:

> *"there is a broad measure of agreement between the Claimants and the Respondents that counsel to the Tribunal can best assist the Tribunal by performing the following roles: (i) identifying documents, parts of documents or gists that ought properly to be disclosed; (ii) making such submissions to the Tribunal in favour of disclosure as are in the interests of the Claimants and open justice; and (iii) ensuring that all the relevant arguments on the facts and the law are put before the Tribunal. In relation to (iii), the Tribunal will expect its counsel to make submissions from the perspective of the Claimants' interests (since the Respondents will be able to make their own submissions). If the Tribunal decides to receive closed oral evidence from one or more of the Respondent's witnesses, it may also direct its counsel to cross-examine them. In practice, the roles performed by counsel to the Tribunal at this stage of the current proceedings will be similar to those performed by a Special Advocate in closed material proceedings."* (Emphasis added)

7.44 In those circumstances, the IPT was plainly right when it rejected the contention that the holding of a closed hearing had been unfair. At §50(ii) of the 5 December judgment it stated:

> *"We do not accept that the holding of a closed hearing, as we have carried it out, is unfair. It accords with the statutory procedure, and facilitates the process referred to in paragraphs 45 and 46 above. This enables a combination of open and closed hearings which both gives the fullest and most transparent opportunity for hearing full arguments inter parties on hypothetical or actual facts, with as much as possible heard in public, and preserves the public interest and national security."*

7.45 Given the Court's conclusions in *Kennedy*, there was clearly no breach of Art. 6 in the approach taken by the IPT.

7.46 **Fourthly** it is said that the IPT refused to hear and decide one of the preliminary issues that was agreed between the parties, namely whether the Respondents'

[161] See the attached submissions of CTT, [***See Annex 62***]
[162] See the IPT's email of 12 September 2014, [***See Annex 63***]

'neither confirm nor deny' ('NCND') policy in relation to the existence of particular interception programmes, was justified. However, as is evident from §13 of the judgment dated 5 December, that issue was, by agreement between the parties, not decided by the IPT:

> *"There were also certain of the Agreed Issues (Issue xii), (xiii) and (xiv) which were described as "Issues of law relating to procedure", and which, by agreement, have not fallen for decision at this hearing. They relate in part to the NCND policy, the importance of which is emphasised by the Respondents in the following paragraphs of their Open Response*[163]*…* (emphasis added)

In those circumstances the Applicants cannot now complain that this issue was

[163] Those open paragraphs of the Response stated:
"5. Secrecy is essential to the necessarily covert work and operational effectiveness of the Intelligence Services, whose primary function is to protect national security. See e.g Attorney General v. Guardian Newspapers Ltd (No.2)[1990] 1 AC 109, per Lord Griffiths at 269F.
6. As a result, the mere fact that the Intelligence Services are carrying out an investigation or operation in relation to, say, a terrorist group, or hold information on a suspected terrorist, will itself be sensitive. If, for example, a hostile individual or group were to become aware that they were the subject of interest by the Intelligence Services, they could not only take steps to thwart any (covert) investigation or operation but also attempt to discover, and perhaps publicly reveal, the methods used by the Intelligence Services or the identities of the officers or agents involved. Conversely, if a hostile individual or group were to become aware that they were not the subject of Intelligence Service interest, they would then know that they could engage or continue to engage in their undesirable activities with increased vigour and increased confidence that they will not be detected.
7. In addition, an appropriate degree of secrecy must be maintained as regards the intelligence-gathering capabilities and techniques of the Intelligence Services (and any gaps in or limits to those capabilities and techniques). If hostile individuals or groups acquire detailed information on such matters then they will be able to adapt their conduct to avoid, or at least minimise, the risk that the Intelligence Services will be able successfully to deploy those capabilities and techniques against them.
8. It has thus been the policy of successive UK Governments to neither confirm nor deny whether they are monitoring the activities of a particular group or individual, or hold information on a particular group or individual, or have had contact with a particular individual. Similarly, the long-standing policy of the UK Government is to neither confirm nor deny the truth of claims about the operational activities of the Intelligence Services, including their intelligence-gathering capabilities and techniques.
9. Further, the "neither confirm nor deny" principle would be rendered nugatory, and national security thereby seriously damaged, if every time that sensitive information were disclosed without authority (i.e. "leaked"), or it was alleged that there had been such unauthorised disclosure of such information, the UK Government were then obliged to confirm or deny the veracity of the information in question.
10. It has thus been the policy of successive Governments to adopt a neither confirm nor deny stance in relation to any information derived from any alleged leak regarding the activities or operations of the Intelligence Services insofar as that information has not been separately confirmed by an official statement by the UK Government. That long-standing policy is applied in this Open Response."
Because this hearing has been held on the basis of agreed assumed facts, it has not been necessary to address this policy or its consequences."

not determined by the IPT.

7.47 Further, and in any event, the Court has itself recognised the importance of the "neither confirm nor deny" approach in maintaining the efficacy of a secret surveillance system, see *Klass* at §58, *Weber* at §135 and *Segerstedt-Wiberg v Sweden*, judgment 6 June 2006 at §102. Significantly in *Kennedy* at §187 the Court accepted that the governments' NCND policy was a valid basis on which eg. documents submitted to the IPT would be highly sensitive and therefore incapable of being disclosed.

7.48 In those circumstances and given that the IPT gave specific consideration to what information could be disclosed in the proceedings, assisted, as it was in closed, by CTT (see §7 and §10 of the 5 December judgment), there was no failure to consider an issue which could have impacted on the fairness of the proceedings.

7.49 **Fifthly** the Applicants complain that, in finding that the regime was in accordance with the law, it placed significant reliance on secret arrangements which were not disclosed to the Applicants and on which the Government were permitted to make submissions during closed proceedings. The Government repeat the submissions at §§7.41-7.45 above. In short, recourse to closed material was strictly necessary given the national security concerns which arose, but any inroads into the fairness of the proceedings were sufficiently counterbalanced by the independent scrutiny provided by the IPT, with the assistance of CTT in the proceedings.

7.50 **Finally** it is said that the IPT took no steps to ensure that the Applicants were effectively represented in closed proceedings. For the reasons already set out above, this has no merit. CTT was appointed and did represent the Applicants' interests in the closed proceedings, as referred to at §10 of the IPT's 5 December judgment, and as set out at §§7.32-7.35 above.

8 QUESTION 6. ARTICLE 14 OF THE CONVENTION

Whether there has been a violation of Article 14 taken together with Article 8

and/or Article 10 on account of the fact that the safeguards set out in s.16 of RIPA 2000 grants additional safeguards to people known to be in the British Islands?

8.1 The Applicants contend that the s.8(4) Regime is indirectly discriminatory on grounds of nationality contrary to Article 14 ECHR, because persons outside the United Kingdom are *"disproportionately likely to have their private communications intercepted"*[164] and/or because s.16 RIPA grants *"additional safeguards to persons known to be in the British Islands"*; and, it is said, that difference in treatment is not justified.

8.2 The true position is as follows:

(1) The operation of the s.8(4) Regime does not mean that persons outside the United Kingdom are disproportionately likely to have their private communications intercepted. The Applicants' case is factually incorrect.

(2) At the stage when communications are selected for examination, the s.8(4) Regime provides an additional safeguard for persons known to be within the British Islands. The Secretary of State must certify that it is necessary to examine intercepted material by reference to a factor referable to such a person. To that extent, persons are treated differently on the basis of current location.

(3) However, the application of that safeguard to persons known to be within the British Islands, and not to persons outwith the British Islands, does not constitute a relevant difference in treatment for the purposes of Article 14 ECHR.

(4) Moreover, even if it did constitute a relevant difference in treatment for the purposes of Article 14, it would plainly be justified.

What is the relevant difference in treatment, if any?

8.3 The operation of the s. 8(4) Regime does not have the effect of making persons outside the British Islands more liable to have their communications intercepted, than persons within the British Islands. "*External communications*" include those which are sent from outside the British Islands, to a recipient in the British Islands; or

[164] See the Applicants' Additional Submissions, §83.

sent from within the British Islands, to a recipient outside the British Islands. Persons outside the British Islands are therefore not necessarily any more likely than persons within the British Islands to have their communications intercepted under a regime which focuses upon certain types of "*external communication*"; particularly if, as is alleged, the regime operates in relation to fibre optic cables within the British Islands.

8.4 The sole respect in which persons may be treated differently by reason of current location under the s. 8(4) Regime is that at the selection stage, limitations are imposed on the extent to which intercepted material can be selected to be read, looked at or listened to according to a factor which is referable to an individual who is known to be for the time being in the British Islands (for example, by reference to a UK landline telephone number). Before such a course may be taken, the Secretary of State must certify that it is necessary under s.16 RIPA.

8.5 The Applicants contend that this difference in treatment on the basis of current location amounts to a relevant difference in treatment for the purposes of Article 14, saying that it amounts to indirect discrimination on grounds of nationality. That contention is contrary to the ECtHR's case law, which has indicated that mere geographical location at any given time is not a relevant difference in status for the purposes of Article 14: see *Magee v United Kingdom* app. No. 28135/95, ECtHR, 6 June 2000, at §50[165].

8.6 In any event, if, contrary to the above, that difference in current location is a relevant difference in treatment, then it is clearly justified.

Justification

8.7 In assessing whether and to what extent differences in otherwise similar situations justify differential treatment, the ECtHR allows States a margin of appreciation,

[165] The applicant in *Magee* was arrested in Northern Ireland on suspicion of terrorism. He complained that his treatment was contrary to Art 14 because suspects arrested and detained in England and Wales under prevention of terrorism legislation could inter alia have access to a lawyer immediately; and that was not the case in Northern Ireland. The Court said that any difference in treatment was *"not to be explained in terms of personal characteristics, such as national origin or association with a national minority, but on the geographical location where the individual is arrested and detained"* and that the difference did not amount to discriminatory treatment within the meaning of Art 14.

which varies according both to the ground for differential treatment, and the subject matter at issue. Thus, a distinction is to be drawn between grounds of discrimination under Art. 14 which *prima facie* appear to offend respect due to the individual (as in the case of sex or race), where severe scrutiny is called for; and those which merely require the State to show that the difference in treatment has a rational justification and is not "manifestly without reasonable foundation": see e.g. *Stec v United Kingdom* app. 65731/01, Grand Chamber, 12 April 2006 at §52. The margin of appreciation is also commensurately greater, where questions of national security are concerned. Thus, to the extent that Art 14 is engaged at all, the present circumstances in which the Government is to be afforded a wide margin of appreciation. It need show only that the differential treatment at issue is not manifestly without reasonable foundation.

8.8 There is plainly a rational justification for treating persons known to be in the British Islands, and persons not known to be in the British Islands, differently under s. 16 of RIPA, as the IPT rightly found in the Liberty proceedings.

8.9 The Government has considerable powers and resources to investigate a person within the British Islands, without any need to intercept their communications under a s. 8(4) warrant. See *Farr* §§145-146. For instance, the Security Service can search their details against open source information; make enquiries with a local police force; deploy surveillance against the person's address; and apply to major telephone and internet service providers for a "*subscriber check*" to determine the name of any subscriber for telephone and broadband services at that address. Once a broadband line has been identified, that specific line can be intercepted. All these factors explain why it should generally be feasible to intercept the communications of a person within the British Islands through a warrant under s.8(1) RIPA naming that person, or their property, and setting out in a schedule the factors to be used to identify the communications to be intercepted.

8.10 That being so, the circumstances in which it is necessary to attempt to obtain the communications of a person in the British Islands under a s. 8(4) warrant should be relatively rare. So it is practicable and proportionate for the Secretary of State to

consider each such instance, and (if appropriate) certify that this is indeed necessary under s. 16(3) RIPA:

(1) As a matter of proportionality, it is important to consider whether the communications could be obtained by other, more specifically targeted, means; and
(2) Selection of material obtained under a s. 8(4) warrant should not be used as a means of evading the type of controls in s. 8(1) of RIPA.

8.11 Conversely, the Government will not usually have anything like the same powers to investigate a person outside the British Islands, without the use of a s. 8(4) warrant. So the circumstances in which the Government will need to examine material obtained under a s. 8(4) warrant for the purpose of obtaining the communications of specific individuals outside the British Islands are commensurately wider. That is sufficient justification for treating the two cases differently.

8.12 The Applicants nevertheless assert that differential treatment cannot be justified, because GCHQ is able to exercise an "*identical degree of control*" over all communications passing through fibre optic cables that they intercept, whether they be between Birmingham and London, or Toronto and Cairo: Additional Submissions, §84.

8.13 **First,** that analysis ignores the fact that the Government has a panoply of powers to investigate a person in Birmingham, which it does not have to investigate a person in Cairo. In general, the Government should be able to investigate an identifiable Birmingham-based individual without the need to examine data obtained under a s. 8(4) warrant at all; not so for the individual in Cairo.

8.14 **Secondly,** it assumes that the Intelligence Agencies are likely to have the same base of knowledge from which to identify the communications of a person in Cairo, as they would have for a person in Birmingham. That assumption is wholly unjustified. Because the Government does not have the same powers to investigate individuals outside the British Islands, it may not know exactly who the individual in Cairo is; or may have an online identity for him, without a name; or may have a variety of

aliases, without knowing his true identity. Yet the logic of the Applicants' position is that in all such cases, the use of any combination of factors for the purpose of identifying communications from or to the individual in Cairo would have to be certified by the Secretary of State, because any such factors would be "referable" to him.

8.15 **Thirdly,** it ignores the fact that the number of cases in which it is necessary to identify the communications of individuals in the British Islands using a s. 8(4) warrant are relatively rare by comparison with the communications of individuals outside the British Islands, for all the reasons set out above. So the questions of practicality that would arise, were it necessary for the Secretary of State to certify all factors relating to such individuals, are commensurately much more acute.

8.16 Put another way, on the Applicants' case, if one were interested in the communications from or to (say) a thousand British Jihadists in Syria and Northern Iraq, use of any factor or combination of factors that was designed to elicit communications from or to any individual Jihadist would require consideration by, and consequent certification from, the Secretary of State. Whether or not that would make the entire selection process unworkable, it indicates at the very least why there is a rational justification for treating persons *"for the time being in the British Islands"* differently under s. 16(2), from persons not in the British Islands.

Anna McLeod

Anna McLeod

18 April 2016 (Agent of the Government of the United Kingdom)

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 2

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION,

Plaintiff,

v.

NATIONAL SECURITY AGENCY / CENTRAL SECURITY SERVICE, *et al.*,

Defendants.

No. 1:15-cv-00662-TSE

DECLARATION OF JONATHON PENNEY

TABLE OF CONTENTS

I. QUALIFICATIONS

1. I am an Associate Professor at the Schulich School of Law and Director of the Law & Technology Institute at Dalhousie University, located in Halifax, Canada. I submit this declaration in support of Plaintiff Wikimedia Foundation's ("Wikimedia's") Opposition to Defendants' Motion for Summary Judgment. Unless otherwise stated, I have personal knowledge of the facts herein.

2. I am a legal academic and social scientist. I hold a DPhil (Ph.D.) in Information, Communication, and the Social Sciences and an M.S.T. in Legal Research from the University of Oxford, as well as an L.L.M. from Columbia Law School, and a J.D. and B.A. from Dalhousie University.

3. I have extensive experience in the scientific study of social phenomena, specifically as it relates to online behavior. During my doctoral studies at Oxford, I received substantial training in empirical, statistical, and social science methods. In addition to my professorship, I also hold appointments at leading research centers in my field. I am currently a Research Fellow at the Citizen Lab, located at the University of Toronto's Munk School of Global Affairs and Public Policy; a Research Associate of Princeton's Center for Information Technology Policy and the Civil Servant Project at the Massachusetts Institute of Technology's Media Lab; and was formerly a Berkman Fellow and Research Affiliate at the Berkman Klein Center for Internet & Society at Harvard University.

4. I have a deep understanding of "chilling effects" theory—the idea that laws, surveillance, or other regulatory actions may "chill" or deter individuals from exercising their rights or freedoms. A central focus of my doctoral dissertation at Oxford was the study of Internet surveillance-related chilling effects. I collected and analyzed data that showed increased public

awareness of National Security Agency ("NSA") surveillance practices resulted in a reduction of privacy-sensitive Wikipedia article page views, and concluded this reduction was evidence of a statistically significant "chilling effect."

5. My doctoral dissertation, which included this Wikipedia "chilling effects" study, was peer reviewed by two examiners for my doctoral thesis defense at the University of Oxford in November 2015. The examiners were Urs Gasser, Professor at Harvard Law School and Executive Director of Harvard University's Berkman Klein Center for Internet and Society, and Joss Wright, Senior Research Fellow at the Oxford Internet Institute, University of Oxford, and a Turing Fellow at the Alan Turing Institute, the United Kingdom's national institute for data science and artificial intelligence. The thesis, which included the study, was successfully defended and accepted with no corrections. The study was also formally peer reviewed, and a draft paper based on it accepted for presentation, by members of the Program Committee for the Inaugural Society for Empirical Legal Studies (SELS) Global Junior Empirical Legal Scholars Workshop in December 2015. The Program Committee reviewed all submissions and selected the best papers for presentation at the workshop. The Program Committee included some of the leading empirical legal scholars internationally, including David Abrams, Professor of Law, Business Economics, and Public Policy at University of Pennsylvania Law; Bernie Black, the Nicholas D. Chabraja Professor at Northwestern University School of Law; Valarie Hans, Professor at Cornell Law School; and Eyal Zamir, Augusto Levi Professor of Commercial Law and Director of the Center for Empirical Studies of Decision Making and the Law at Hebrew University.

6. Informally, the study was also peer reviewed by computational social scientist Nathan Matias in May 2016, who at the time was a doctoral candidate at the Massachusetts Institute of Technology's Media Lab and is now a Post-Doctoral Research Associate at Princeton University,

cross-appointed in Princeton's Psychology Department, Sociology Department, and the Center for Information Technology Policy. In addition, Matthew Salganik, Professor in the Department of Sociology at Princeton University, has reviewed the study, using it as part of course materials for his class, "Computational Social Science: Social Research in the Digital Age," at Princeton University's Sociology Department. He has also cited the study multiple times in his leading text on computational social science research and methods.[1]

7. The study was also informally peer reviewed via numerous presentations to faculty, academic researchers, graduate students, and a range of other experts in 2015 and 2016, including Harvard University's Berkman Klein Center for Internet and Society in May 2015 and April 2016; and the 5th Annual Workshop on Free and Open Communications on the Internet (FOCI) Workshop, USENIX Security Symposium, Advanced Computing Systems Association (ACSA), Washington, D.C. in August 2015.

8. In 2016, I published the findings from my doctoral research in the *Berkeley Technology Law Journal*. I have also published other research on chilling effects and online privacy in peer-reviewed data science and policy journals. My statement of qualifications, including my professional curriculum vitae and list of publications, is attached as Appendix B.

II. ASSIGNMENT

9. Wikimedia has retained me to provide expert consultation, analyses, and testimony in the lawsuit *Wikimedia Foundation v. National Security Agency, et al.*, No. 1:15-cv-00662-TSE (D. Md.). My assignment is to provide opinions on the chilling effects associated with "Upstream" Internet surveillance conducted by the Defendant National Security Agency ("NSA"). Neither

[1] *See* MATTHEW SALGANIK, BIT BY BIT: SOCIAL RESEARCH IN THE DIGITAL AGE (2017).

Wikimedia nor anyone else is compensating me for this work, and my participation is not dependent on the opinions provided or the outcome of the case.

III. SUMMARY OF OPINIONS

10. Based on the empirical evidence and my statistical analysis, I conclude that public awareness of NSA surveillance programs, including Upstream surveillance, which became widespread during the June 2013 Snowden disclosures, is highly likely to have had a large-scale chilling effect on Wikipedia users.

11. I arrive at this conclusion based on (1) the statistically significant and substantial drop in view counts immediately following June 2013 for Wikipedia articles that would likely raise privacy concerns for users aware of NSA Internet surveillance; (2) the statistically significant trend reversal in monthly views for those articles after June 2013, which indicates a sustained impact on viewership that did not course correct after this revelation; and (3) the lack of comparable statistically significant reductions and reversals in monthly article views for comparator Wikipedia articles over the same time period.

IV. OVERVIEW OF CHILLING EFFECTS THEORY & SUPPORTING EMPIRICAL EVIDENCE FOR SURVEILLANCE RELATED CHILL ONLINE

12. Chilling effects theory posits that government surveillance can harm individuals by "chilling" or deterring them from exercising their rights and freedoms out of fear of legal punishment, social sanction, or to avoid invasions of privacy and reputational risks. There is an extensive body of legal scholarship establishing the underpinnings of chilling effects theory.[2]

[2] *See generally* Frederick Schauer, *Fear, Risk, and the First Amendment: Unraveling the "Chilling Effect,"* 58 B.U. L. REV. 685 (1978) (the leading academic account of chilling effects theory); Daniel Solove, *A Taxonomy of Privacy*, 154 U. PENN. L. REV. 477 (2006) (analyzing theory in the context of modern surveillance practices and data gathering, focusing on how government surveillance of online activities creates a broader atmosphere of conformity and self-censorship).

13. Some social science research has indicated that self-reported or expressed concerns about privacy do not necessarily reflect people's actual behavior online, a phenomenon sometimes referred to as the "privacy paradox."[3] However, especially in recent years, empirical studies have tested and confirmed the tenets of chilling effects theory as they apply to online behavior, including specifically as it relates to online government surveillance.

14. Social science research and empirical studies have been conducted that demonstrate online behavior is chilled as a result of government surveillance. Importantly, multiple studies confirm specifically that public awareness surrounding NSA surveillance activities, including Upstream surveillance, created a chilling effect online. *See also infra* Part V.A.i (establishing significance of public awareness and shock created by media coverage of the Snowden disclosures).

15. A Massachusetts Institute of Technology (MIT) study on Google search traffic by Alex Marthews and Catherine Tucker, later published in 2017 as a peer reviewed chapter in the Cambridge University Handbook on Surveillance Law, found a statistically significant 4% reduction in Google searches after the June 2013 Snowden disclosures for certain search terms that would raise privacy concerns for Internet users aware of NSA surveillance online.[4] This finding, that awareness of online surveillance chilled Internet users from searching for certain topics and content, strongly supports the conclusions I draw herein. It also provides additional evidence that

[3] *See* Spyros Kokolakis, *Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon*, COMPUTERS & SOC'Y 1 (2015) (providing a comprehensive explanation and review of "information privacy paradox" literature).

[4] Alex Marthews & Catherine Tucker, *Government Surveillance and Internet Search Behavior*, *in* CAMBRIDGE UNIVERSITY HANDBOOK ON SURVEILLANCE LAW (David Gray et al. eds., 2017).

Internet users were generally aware of NSA surveillance starting as of June 2013, and it impacted their online activities.

16. Elizabeth Stoycheff's 2016 experimental study, later published in a peer reviewed article entitled "Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring," found that exposing participants to "terms of agreement," which reminded participants that their online activities could be subject to interception and surveillance, chilled those participants from expressing their political views, especially those participants who believed their political views were controversial or less popular.[5] Again, this chilling effect, due to awareness of online surveillance, is consistent with findings from my own observational study.

17. Andrea Forte et al.'s 2017 qualitative study on Wikipedia editors, published in a peer reviewed paper entitled "Privacy, Anonymity, and Perceived Risk in Open Collaboration: A Study of Tor Users and Wikipedians," found evidence that editors were chilled from certain activities on Wikipedia due to awareness of government surveillance.[6] For example, one Wikipedia editor stated that surveillance "has a chilling effect on the way that we do business and on the ability which Wikipedia has, [as] an enterprise, to continue. Because people are far less likely to engage with us, if they know that the American government is watching their every move." Another Wikipedia editor confirmed these chilling effects, stating, "for the Edward Snowden page, I have pulled myself away from adding sensitive contributions, like different references, because I thought the name may be traced back to me in some way." These findings are also consistent with my conclusions about chilling effects on Wikipedia use.

---

[5] Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, 93(2) JOURNALISM & MASS COMMUNICATION 296 (2017).

[6] Andrea Forte, Nazanin Andalibi, and Rachel Greenstadt, *Privacy, Anonymity, and Perceived Risk in Open Collaboration: A Study of Tor Users and Wikipedians*, in CSCW 1800 (2017).

18. A series of survey-based empirical studies of Americans published by PEW Research Center in 2013, 2014, and 2015 found people were chilled in their online activities due to their awareness of government surveillance programs after June 2013.[7] A Pew Research Center survey of 475 adult Americans conducted between November 26, 2014 and January 3, 2015, and published in a report entitled "Americans' Privacy Strategies Post-Snowden" in March 2015, found 87% of respondents were aware of "government surveillance programs to monitor phone use and internet use" due to the Snowden disclosures. Among that 87%, 34% had taken "at least one step to hide or shield their information from the government" such as changing privacy settings, using social media less, avoiding certain apps, speaking more in person than online, and avoiding using "certain terms in online communications." It also found 25% changed the patterns of their own use of various technological platforms "a great deal" or "somewhat" since the Snowden revelations. Similarly, a survey of 1,801 adults conducted between August 7-September 16, 2013, and published in a report entitled "Americans' Privacy Strategies Post-Snowden" in August 2014, found that survey respondents were less willing to discuss the "Snowden-NSA story" online "than they were in person" with 86% indicating they would speak about the story "in person" but only 42% would speak about it on social media. Again, a July 2013 survey of 1,002 American adults ages 18 and older, published in a report entitled "Anonymity, Privacy, and Security Online" in September 2013, found 86% tried to use the Internet in ways to minimize the visibility of their digital footprints, including 55% saying that had "used the internet in ways to

[7] KEITH N. HAMPTON ET AL., PEW RES. CTR., SOCIAL MEDIA AND THE 'SPIRAL OF SILENCE,' 4 (2014), http://www.pewinternet.org/files/2014/08/PI_Social networks and debate_082614.pdf; LEE RAINIE ET AL., PEW RES. INTERNET PROJECT, AMERICANS' PRIVACY STRATEGIES POST-SNOWDEN 4 (Mar. 16, 2015), http://www.pewinternet.org/files/2015/03/PI_AmericansPrivacyStrategies_0316151.pdf; Lee Rainie et al., *Anonymity, Privacy, and Security Online*, Pew Res. Ctr. (2013), http://www.pewinternet.org/2013/09/05/anonymity privacy and security online.

avoid being observed or seen" by a range of people, groups, and institutions, including government and law enforcement. All of these studies are consistent with the results of my empirical study of Wikipedia page view traffic. They also critically support June 2013 as the initial date that people became aware of NSA surveillance activities, including Upstream surveillance.

19. A PEN American Center study of writers in 2013 and 2015 also found evidence of chilling effects associated with awareness of government surveillance after the Snowden revelations in June 2013.[8] The October 2013 survey of 520 American writers, later published in a report entitled "Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor" in November 2013, found that 28% of the writers surveyed had "curtailed or avoided" certain online activities due to "fear of surveillance" and another 12% "seriously considered" doing so; 24% "deliberately avoided certain topics in phone or email conversations," and another 9% have "seriously considered it"; and 16% have refrained from "conducting Internet searches or visiting websites on topics that may be considered controversial or suspicious," and another 12% have "seriously considered it." A second PEN American survey of 772 international writers living in 50 countries, conducted from August to October 2014 and later published in a report entitled "Global Chilling: The Impact of Mass Surveillance on International Writers" in January 2015, found 34% of writers living in "free countries" have "avoided writing or speaking on a particular topic, or have seriously considered it, due to fear of government surveillance," and another 42% have "curtailed or avoided activities on social media, or seriously considered it, due to fear of

[8] FDR GROUP & PEN AMERICAN CENTER, CHILLING EFFECTS: NSA SURVEILLANCE DRIVES U.S. WRITERS TO SELF-CENSOR 3–4 (2013), http://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf; FDR GROUP & PEN AMERICAN CENTER, GLOBAL CHILLING: THE IMPACT OF MASS SURVEILLANCE ON INTERNATIONAL WRITERS (2015), http://www.pen.org/sites/default/files/globalchilling_2015.pdf.

government surveillance." Again, these findings are consistent with my conclusions here concerning chilling effects on Wikimedia users.

20. Other recent qualitative and quantitative studies also document how government surveillance has a chilling effect on various online and offline activities. Karin Wahl-Jorgenson et al.'s qualitative and quantitative study of how surveillance impacts U.K. journalists, published in a peer-reviewed paper in 2017, found "many" journalists interviewed "cited personal experience with surveillance" and how it has had a "chilling effect on reporting practices."[9] Lina Dencik and Jonathan Cable's qualitative study involving focus groups and interviews among journalists and activists in the United Kingdom, and published in a peer-reviewed journal in 2017, found evidence of surveillance chilling effects among participants "both for ordinary communication and for pursuing particular forms of social change or expressing dissent."[10] Paul Lashmar's study involving interviews with journalists after the Snowden revelations, published in a peer reviewed journal in 2017, found all participants believed the existence of mass government surveillance would "chill" and deter confidential sources from speaking with journalists.[11] Additionally, Margot Kaminski and Shane Witnov's 2015 law review article cites a range of other social science

[9] Karin Wahl-Jorgensen, Lucy K. Bennett, & Jonathan Cable, *Surveillance Normalization and Critique: News coverage and journalists' discourses around the Snowden revelations*, 5(3) DIGITAL JOURNALISM 386 (2017).

[10] Lina Dencik and Jonathan Cable, *The Advent of Surveillance Realism: Public Opinion and Activist Responses to the Snowden Leaks*, 11 INTERNATIONAL JOURNAL OF COMMUNICATION 763 (2017).

[11] Paul Lashmar, *No more sources? The impact of Snowden's revelations on journalists and their confidential sources*, 11(6) JOURNALISM PRACTICE 665 (2017).

research to support the assumption that surveillance has a chilling effect on speech and other behavior.[12]

21. Finally, my own survey-based study of over 1200 American Internet users, published in a peer-reviewed journal in 2017, found that awareness of possible government online surveillance has a chilling effect on a range of online activities, including 62% of participants being much less likely or somewhat less likely to "speak or write about certain topics online"; 78% indicating they would be "more careful" about what they "search for online"; and 60% being much less or somewhat less likely to share personally created content online, among other findings.[13] I also found that participants with greater awareness of news about the NSA were statistically more chilled by government surveillance. All of these studies, and their findings, support my conclusions here concerning chilling effects on Wikimedia users.

V. WIKIPEDIA STUDY—DESIGN, METHOD, AND RESULTS

22. As part of my doctoral research at Oxford, I designed an empirical study to test chilling effects theory, focusing on Internet user interaction with Wikipedia, one of the world's most viewed websites and an important source knowledge and information for people around the globe. The study examined Wikipedia article page view traffic before and after June 2013, to test the hypothesis that increased public awareness about NSA surveillance would lead to users being less likely to view Wikipedia articles on certain privacy-sensitive topics. This Part summarizes the study's design, methodology, and findings.

---

[12] *See* Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 465, 480 (2015).

[13] Jonathon Penney, *Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study*, 6(2) INTERNET POLICY REVIEW (2017).

A. Design

23. My design emphasizes a quasi-experimental approach—commonly accepted in social science—to understanding the impact of NSA surveillance activity on user behavior—studying behavior both immediately following the June 2013 revelations, described as "level" changes, and the longer-term rates of viewership, described as "trend" changes. Combined, the decrease in level and trend constitute the full "chilling effect" of NSA surveillance.

24. To test my hypothesis, I used the most robust experimental design available given the available information and context around the NSA surveillance revelations. The "gold-standard" approach, randomized control trials, for definitive proof of a causal relationship between the NSA activity and viewership is not possible in this instance, as the revelations were widespread and impossible to assign randomly. Thus, I chose a robust quasi-experimental approach common in social science research—an interrupted time series (ITS) design with segmented regression analysis. ITS offers a powerful statistical means to analyze whether page views for privacy-concerning Wikipedia articles were impacted by public awareness about NSA surveillance programs after the June 2013 Snowden revelations.[14] In an ITS design, a series of observations on the same outcome, collected at equally spaced intervals over time, before and after an

[14] For discussion of interrupted time series research design, see DONALD T. CAMPBELL, JULIAN C. STANLEY & NATHANIEL L. GAGE, EXPERIMENTAL AND QUASI-EXPERIMENTAL DESIGNS FOR RESEARCH 37–43 (1966) (discussing the components of time series designs and their methodological advantages and limitations); A.K. Wagner et al., *Segmented Regression Analysis of an Interrupted Time Series in Medication Use Research*, 27 J. CLINICAL PHARMACY & THERAPEUTICS 299 (2002) (discussing advantages of using of segmented regression analysis along with ITS design); Monica Taljaard et al., *The use of segmented regression in analysing interrupted time series studies: an example in pre-hospital ambulance care*, 9 IMPLEMENTATION SCIENCE 1 (2014); Mylene Lagarde, *How to do (or not to do) … Assessing the impact of a policy change with routine longitudinal data*, 27:1 HEALTH POLICY AND PLANNING 76 (2012); Robert B. Penfold & Fang Zhang, *Use of Interrupted Time Series Analysis in Evaluating Health Care Quality Improvements*, 13:6 ACAD. PEDIATRICS S38 (2013) (discussing the advantages and limitations of employing time series analysis to understand and explore the impact of policy changes).

intervention, are used to test the immediate and longer term effect of the intervention.[15] A major strength of the design is its ability to distinguish the impact or effect of an intervention from the "secular" trend, that is, the trend or changes that would have occurred over time but for the intervention.[16]

25. In order to be a valid indicator of causal change, an ITS design requires primarily that the point of "intervention"—in this case public knowledge of NSA surveillance activities—be clear and fairly immediate. The prior research cited above on public awareness supports this date as an unambiguous intervention point to use when testing this hypothesis, and I further lay out evidence of public awareness below. I also conducted ITS segmented regression on "comparator" articles with the same intervention point to further test the ITS approach with reasonable "control" groups, insolating the impacts of the intervention. The effects of an ITS are estimated by comparing both level and trend in the pre- and post-intervention periods through the use of segmented regression. Here, the time period studied before and after the June 2013 revelations is long enough to control for overall trends (for example, seasonality or other long-term changes in page views) and to determine if the decline in page views was temporary or more permanent and damaging. The data after the intervention have a different level and trend than the pre-intervention series, indicating public awareness of NSA surveillance impacted users' Wikipedia use.

i. Intervention Selection

26. On June 6, 2013, stories in The Guardian and *The Washington Post* detailed previously undisclosed information and leaked classified documents about the surveillance practices of the

[15] Taljaard, *id.*; Lagarde, *id.*

[16] Taljaard, *id.*

United States and other Western governments.[17] The June 2013 revelations (also, "Snowden revelations") were followed by stories in June and subsequent months covering a vast array of government surveillance practices and operations.[18]

27. The revelations caused a "media and political storm," receiving widespread coverage both in traditional and new media outlets, and sparking a "heated international debate" in the United States, Europe, Russia, and beyond.[19]

28. Governments cited the "War on Terror" to defend the surveillance programs, and this justification was reflected in media coverage of the Snowden revelations.[20] The Snowden leaks and coverage, as media scholar Vian Bakir has noted, highlighted the previously limited public awareness about government surveillance activities while also augmenting that awareness.[21]

29. Indeed, in the United States, the widespread media coverage has led to greater awareness and concern among the general public about government surveillance activities and

---

[17] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 6, 2013), http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secretprogram/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497story.html; Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[18] *See* David Lyon, *Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique*, 1 BIG DATA & SOC'Y 1, 2 (2014) (discussion and analysis of subsequent news stories covering surveillance revelations).

[19] Vian Bakir, *Agenda Building, and Intelligence Agencies: A Systematic Review of the Field from the Discipline of Journalism, Media, and Communications*, 20 INT'L J. PRESS/POL. 131 (2015).

[20] *Id*. at 133; *see* Jie Qin, *Hero on Twitter, Traitor on News: How Social Media and Legacy News Frame Snowden*, 20 INT'L J. PRESS/POL.166 (2015) (finding that a predominant "framing" in traditional news media coverage of the Snowden surveillance disclosures focused on national security terrorism, along with international relations).

[21] *See* Bakir, *supra* note 19, at 133.

anti-terrorism efforts more generally. A Pew study in 2014 found that 87% of U.S. adults had heard something about "the government collecting information about telephone calls, e-mails, and other online communications" as part of "efforts to monitor terrorist activity" (with 43% hearing "a lot" and 44% hearing "a little"); another 80% agreed or strongly agreed that "Americans should be concerned" about government surveillance.[22] This increased awareness of online government surveillance presented a unique opportunity for chilling effects research. The surveillance revelations and widespread surrounding publicity constituted an "exogenous shock," or focal point, to study the effects of surveillance on Internet use behavior.

30. I examined view count data for privacy-sensitive Wikipedia articles before and after June 2013, to see if the greater awareness about potential NSA surveillance online may have "chilled" or deterred Internet users from viewing such privacy-sensitive content on Wikipedia. In other words, I tested the following hypothesis: due to chilling effects caused by increased awareness of NSA surveillance online, including Upstream surveillance, Internet users will be less likely to view Wikipedia articles on topics that raise privacy-related concerns.

ii. Data Selection

31. To select privacy-sensitive Wikipedia articles to track in the study, I matched 48 Wikipedia articles with a list of "terrorism" related keywords that the U.S. Department of Homeland Security (DHS) uses to track and monitor social media.[23] This DHS keyword list

[22] MARY MADDEN, PUBLIC PERCEPTIONS OF PRIVACY AND SECURITY IN THE POST-SNOWDEN ERA, PEW RES. INTERNET PROJECT 2–3 (Nov. 12, 2014), http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf.

[23] The keyword list has been publicly available online since 2012, and was updated and re-posted by the DHS in 2013: U.S. DEP'T OF HOMELAND SEC., NATIONAL OPERATIONS CENTER MEDIA MONITORING CAPABILITY ANALYST'S DESKTOP BINDER (2011), https://epic.org/foia/epic-v-dhs-media-monitoring/Analyst-Desktop-Binder-REDACTED.pdf. This was later updated and posted online by the DHS. *See* U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE OFFICE OF

categorizes certain search terms or keywords in relation to a range of different issues such as "Health Concern," "Infrastructure Security," and "Terrorism." Forty-eight Wikipedia articles were included in the study that corresponded with DHS keywords listed as relating to "terrorism" ("Terrorism Wikipedia Article Group").[24] The Terrorism Wikipedia Article Group included articles on "dirty bomb," "suicide attack," "nuclear enrichment," and "eco-terrorism," among others.[25] Keywords relating to "terrorism" were used because the U.S. Government cited terrorism as a key justification for its online surveillance practices and media coverage largely framed the Snowden revelations around terrorism and national security.[26]

32. The DHS keyword list was used for pragmatic methodological reasons, that is, a non-random means to select groupings of Wikipedia articles. It was hypothesized that Wikipedia articles coinciding with these terrorism-related topic keywords may include the kind of information or content users may avoid accessing in light of potential government surveillance. To test that hypothesis, a survey of 415 independent Internet users was also conducted to provide additional evidence that Wikipedia articles associated with these "terrorism" keywords raised

---

OPERATIONS COORDINATION AND PLANNING (2013), https://www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy_pia_ops_NOC%20MMC%20Update_April2013.pdf.

[24] Locating Wikipedia articles coinciding with each keyword was done manually; there was a Wikipedia article that corresponded perfectly with the vast majority of keywords in the "terrorism" DHS keyword category. There were a few discrepancies, however: the Wikipedia article "environmental terrorism" was used for the keyword "environmental terrorist"; the keyword "target" was excluded as they were too many potentially corresponding Wikipedia articles; the Wikipedia article "political radicalism" was used for the DHS keyword "radicalism" because there were too many potentially corresponding articles; the keyword "enriched" was excluded as it was redundant with the included Wikipedia article "nuclear enrichment"; and there were also no Wikipedia articles corresponding with DHS keywords "weapons cache," "suspicious substance," "plot," and "homegrown." Wikipedia articles corresponding with the remaining 48 DHS "terrorism"-related keywords were all included in the study.

[25] *See infra* Appendix A, Table 11 ("48 Terrorism Article Group" list), Table 12 (privacy-sensitive score for each of 48 articles).

[26] *See supra* note 20.

privacy concerns for Internet users aware of government surveillance online. Respondents in the survey were recruited through Amazon's Mechanical Turk ("MTurk"), a platform researchers have used to carry out a range of empirical and social science research, including survey research.[27]

33. A total of 415 independent Internet users participated in the crowdsourcing project through MTurk, and they rated each of the 48 topics to which the Wikipedia articles in the data set corresponded. The survey questions were designed to explore the likelihood that the topics would raise privacy-related concerns for Internet users.[28] To minimize self-selection and response bias (a limitation difficult to avoid in non-random sampling), the brief questionnaires were described as merely an "Online Information Study" to potential MTurk participants. The results from the survey are set out in Table 10 and Table 12 of Appendix A.

iii. Data Collection

34. Having selected the 48 Terrorism Wikipedia Articles Group, the study aggregated Wikipedia article view count data on a monthly basis for these Wikipedia articles over a 32-month period, from the beginning of January 2012 to the end of August 2014. The study used data for English language article view counts from stats.grok.se, an online portal that provided access to non-mobile Wikipedia article view count data on a daily and monthly basis, and which was based

[27] Gabriele Paolacci & Jesse Chandler, *Inside the Turk: Understanding Mechanical Turk as a Participant Pool*, 23:3 CURRENT DIRECTIONS PSYCHOL. SCI. 184, 186 (2014), http://cdp.sagepub.com/content/23/3/184.abstract; Matthew J.C. Crump, John V. McDonnell & Todd M. Gureckis, *Evaluating Amazon's Mechanical Turk as a Tool for Experimental Behavioral Research*, 8:3 PLOS ONE e57410, e57410 (2013), http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0057410.

[28] Respondents were asked to indicate on a scale of 1 to 5 (1 being very unlikely and 5 being very likely): how likely they thought they would be in trouble if the U.S. government found out that they accessed information about the topic in question (Government Trouble Rating); how "privacy-sensitive" they viewed each topic as (in this case, 5 being highly sensitive and 1 not at all) (Privacy-Sensitive Rating); how likely they would be to delete the browser history on their computer after accessing information about the topic (Browser Delete Rating); and how likely they would avoid viewing or accessing information on the topic if they knew the Government was monitoring people's activities online (Avoidance Rating).

on a Wikimedia maintained page view dataset. The portal has been used in a range of peer-reviewed research.[29] These Wikipedia article views, or "page views," represent the number of times a Wikipedia article was "requested" from Wikimedia's servers (such as by a non-mobile web browser user clicking on a link to load the Wikipedia article).[30] The Terrorism Wikipedia Articles generated nearly 81 million total page views over the course of the 32-month study period.

B. Method of Analysis

35. A strength of an ITS design is that there are multiple measures before and after the intervention in the time series; such multiplicity controls for changes in level and trends in the data and increases the robustness of results.[31] Thus, my study used Wikipedia article view counts to create a time series over a 32-month period from January 2012 to August 2014 (n=32), with the June 2013 NSA surveillance revelations as the "intervention" that interrupts the time series, dividing it into two segments: before and after June 2013. The study also isolated the impact and lasting effect of the intervention by similarly analyzing the level and trend data for "comparator" Wikipedia articles groups.

---

[29] Research has included studies involving market trends, health information access, and social-political change, among others. *See, e.g.*, Michela Ferron & Paolo Massa, *WikiRevolutions: Wikipedia as a Lens for Studying the Real-Time Formation of Collective Memories of Revolutions*, 5 INT'L J. COMM. 1313 (2011) (examining Wikipedia as a "lens" through which to understand real-time social and political upheaval and change); Michaël R. Laurent & Tim J. Vickers, *Seeking Health Information Online: Does Wikipedia Matter?* 16:4 J. AM MED. INFORMATICS ASS'N 471 (2009) (using Wikipedia traffic data from stats.grok.se to study the relevance of Wikipedia to how people access to health information online); Helen Susannah Moat et al., *Quantifying Wikipedia Usage Patterns Before Stock Market Moves*, 3 SCI. REP. 1 (2013) (investigating Wikipedia article traffic and usage in relation to stock market changes).

[30] The raw Wikipedia article page view statistics track total views or loads of the Wikipedia articles or pages in question, not unique visitors. *See Pageview Statistics*, WIKIPEDIA.ORG, https://en.wikipedia.org/wiki/Wikipedia:Pageview_statistics.

[31] *See* CAMPBELL, STANLEY & GAGE, *supra* note 14, at 37; Lagarde, *supra* note 14; Penfold & Zhang, *supra* note 14, at S39; Wagner et al., *supra* note 14, at 308.

36. Two statistical approaches were used to analyze the interrupted time series. I first conducted a simple comparison of the mean number of views for all the Wikipedia articles in the dataset before and after June 2013. Second, I used a segmented regression analysis to estimate article view trends for the pre/post time segments. The results are reported and analyzed in what follows, with statistically significant findings tabulated and presented graphically.[32]

37. Autocorrelation is the tendency for observations taken over a period of time to be correlated or related to each other. It can be a potentially confounding factor for statistical results arrived at through an ITS design.[33] My study corrected for auto-correlation using the Prais-Winsten method for the second set of results described below—the 47 Wikipedia Terrorism Article Group—and one comparator group, the 34 infrastructure-related Article Group.[34] *See infra* Part C.ii-iii (results for these two sets of article groups).

---

[32] A statistically significant result is a result that is not attributed to random chance. Statistical hypothesis testing is used to determine whether the result of a data set is statistically significant. This test provides a probability value or *p*-value, which represents the probability that random chance could explain the result. Generally, a *p*-value of 0.05 or lower is considered to be statistically significant. It means there is a less than 5% chance that the results are explained by chance, and thus this low probability means we can reject to "null" hypothesis, which assumes that any effect or result is due to chance. A *p*-value of 0.01 or lower, which means there is a less than 1% chance that the results are explained by chance, is considered to be highly statistically significant. John Concato & John A Hartigan, *P values: from suggestion to superstition*, 64 JOURNAL OF INVESTIGATIVE MEDICINE 1166, 1166–67 (2016); Valen E. Johnson, *Revised standards for statistical evidence*, 110:48 PNAS 19313, 19313, 19316 (2013) (describing the "classical hypothesis tests", including "highly significant" p-value level at 0.01); David M. Lane, *Significance Testing*, in (David M Lane, ed.) ONLINE STATISTICS EDUCATION: AN INTERACTIVE MULTIMEDIA COURSE OF STUDY 376, 376–77 (2018), http://onlinestatbook.com/Online_Statistics_Education.pdf.

[33] The Durbin-Watson Test Statistic provides a diagnostic test for autocorrelation. *See* Lagarde, *supra* note 14 at 77, 79. A general rule of thumb is a Durbin-Watson Test result of 1.5 to 2 discloses no autocorrelation concern, while a result closer to 1 (or less) or 3 (or more) may suggest autocorrelation. *See* W. PAUL VOGT & R. BURKE JOHNSON, A DICTIONARY OF STATISTICS & METHODOLOGY: A NONTECHNICAL GUIDE FOR THE SOCIAL SCIENCES 118 (2011).

[34] The Durbin-Watson autocorrelation diagnostic test only showed autocorrelation concerns for these two Article Groups. The Prais-Winsten method is the recommended statistically method to control for auto-correlation. *See* Lagarde, *supra* note 14 at 77, 79.

C. Results

38. The results described below provide evidence of a chilling effect associated with the June 2013 public awareness about NSA surveillance programs.

i. First Set of Results: 48 Terrorism Wikipedia Article Group

39. The average monthly views for all 48 Wikipedia articles in the Terrorism Wikipedia Article Group combined show a noteworthy decrease in views after June 2013. Figure 1 illustrates this decline in page views pre- and post- June 2013, over the course of the 32-month period from January 2012 to August 2014.

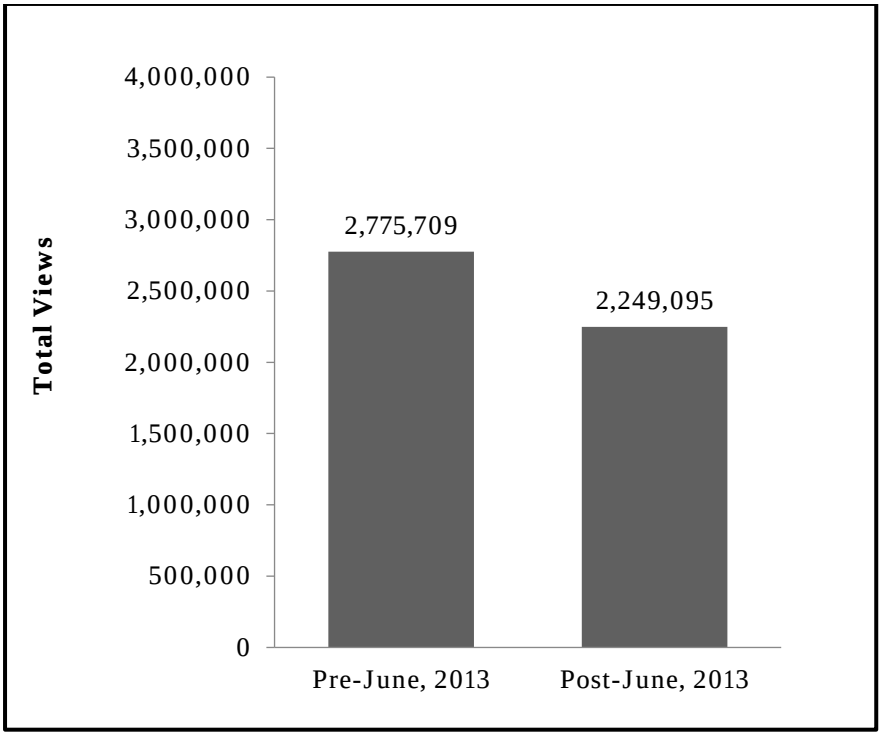


Figure 1. *Average Monthly View Counts, Pre- and Post- June 2013. The reduction after the June 2013 surveillance revelations is consistent with a chilling effect.*

40. The difference in mean monthly page views before and after June 2013 is notable—a reduction of 526,614 in the average monthly views for the articles, which represents approximately

a 19.5% drop in article view counts. This difference is statistically significant[35] and consistent with a chilling effect. To strengthen this inference, further analysis was done using segmented regression, a statistical method of analysis that controls for other variables.

41. The results based upon the more robust segmented regression statistical analysis are also consistent with the hypothesized chilling effects. The first set of results (*see* Table 1 of Appendix A) show that, based on the monthly article view trend existing before June 2013, there was a reduction of 995,085 article views in June 2013, which was a large, sudden, and statistically significant drop in the total view counts for the 48 Terrorism Wikipedia Article Group. The predicted article views for the month of June 2013 based on the pre-June monthly article view trends was 3,199,053, meaning the 995,085 reduction represents an immediate drop-off of 31%. The 31% drop in total view counts is consistent with an immediate and noteworthy chilling effect following the June 2013 revelations.

42. The chilling effect conclusion is further strengthened once the "Hamas" Wikipedia article was excluded from the 48 Terrorism Wikipedia Article Group. The Hamas Wikipedia article was a significant outlier,[36] with view counts skyrocketing in November 2012 and July 2014,

---

[35] "Cohen's *d*" is a test used to determine the "effect size" of a difference between two means, that is, whether the difference (as here) is substantial enough to be meaningful. It is calculated by dividing the means by the standard deviation. A result of 0.8 or more is considered a large effect. Here, the Cohen's *d* value was over 1. *See* David M. Lane, *The Difference Between Two Means*, in (David M Lane, ed.) ONLINE STATISTICS EDUCATION: AN INTERACTIVE MULTIMEDIA COURSE OF STUDY 349, 349 (2018), http://onlinestatbook.com/Online_Statistics_Education.pdf.

[36] Model diagnostics identified two influential outlier data points. The first outlier concerned view counts for the Wikipedia articles in the data set in November 2012 (Cooks D value = 0.1644942), and the other was for view counts in July 2014 (Cooks D value = 0.4121233). Examining more closely the view counts for the entire 48 Wikipedia articles in group, the Hamas article stood out: it had view counts of 928,533 for November 2012, and then 1,220,490 for July 2014, which are far beyond the mean number of view counts for the article across all months in the study (134,574 monthly views). If we exclude these two outlier months, the contrast between the view counts for the Hamas article during those two months and other months in the dataset is even starker, with the mean being 71,912. An assessment that these view counts were outliers is confirmed by the z-scores for those two data points (3.01 and 4.11, respectively).

which corresponded with Gaza conflicts between Hamas and the Israeli Defense Force during those months.[37] Once this single Wikipedia article was excluded, an even clearer picture emerged from the data.

ii. Second Set of Results: 47 Wikipedia Terrorism Article Group (Without Hamas Outlier)

43. Similar to the first set of results, this second set of results (set out in Table 2 of Appendix A) for the 47 Terrorism Wikipedia Article Group (excluding the Hamas article outlier) also showed an immediate and statistically significant decrease in view counts following increased public awareness about NSA surveillance in June 2013: an immediate drop of 693,617 total views. Using the predicted 3,034,721 article views for June 2013 based on the pre-June trend, this reduction represents an immediate drop-off of 23%. This similarly sharp and sudden decrease in view counts after June 2013 is consistent with a chilling effect.

44. Importantly, the second results also showed a statistically significant change in the overall trend in the month-to-month views of the 47 Terrorism Wikipedia Articles Group. Rather than increasing on a monthly basis, the page view trend after June 2013 is decreasing. Before June 2013, the data show an increase of 41,421 views per month. After June 2013, the data show a decrease of 67,513 in views per month. This change is important because it means that the public awareness about NSA surveillance programs is associated with a longer term decrease in views

[37] For a "timeline" of the conflict and the IDF operation against Hamas, see *TIMELINE: Israel Launches Operation Pillar of Defense Amid Gaza Escalation*, HAARETZ (Nov. 20, 2012), http://www.haaretz.com/news/diplomacy-defense/timeline-israel-launches-operation-pillar-of-defense-amid-gaza-escalation.premium-1.479284l; Amos Harel, *At the Crossroads of a Gaza Ground Operation*, HAARETZ (Jul. 12, 2014), http://www.haaretz.com/news/diplomacy-defense/.premium-1.604601. The notion that major conflicts, including the Gaza conflicts, draw "significantly higher levels" of activity on the social media platform Twitter is consistent with findings from previous research. *See* Thomas Zeitzoff, John Kelly & Gilad Lotan, *Using Social Media to Measure Foreign Policy Dynamics: An Empirical Analysis of the Iranian–Israel Confrontation (2012–13)*, 52 J. PEACE RES. 368, 372 (2015).

for the Wikipedia articles studied, consistent with a longer term chilling effect; Figure 3 illustrates this trend. Figure 2 below illustrates both the statistically significant drop off and shift in the overall trend in the view count data after June 2013.

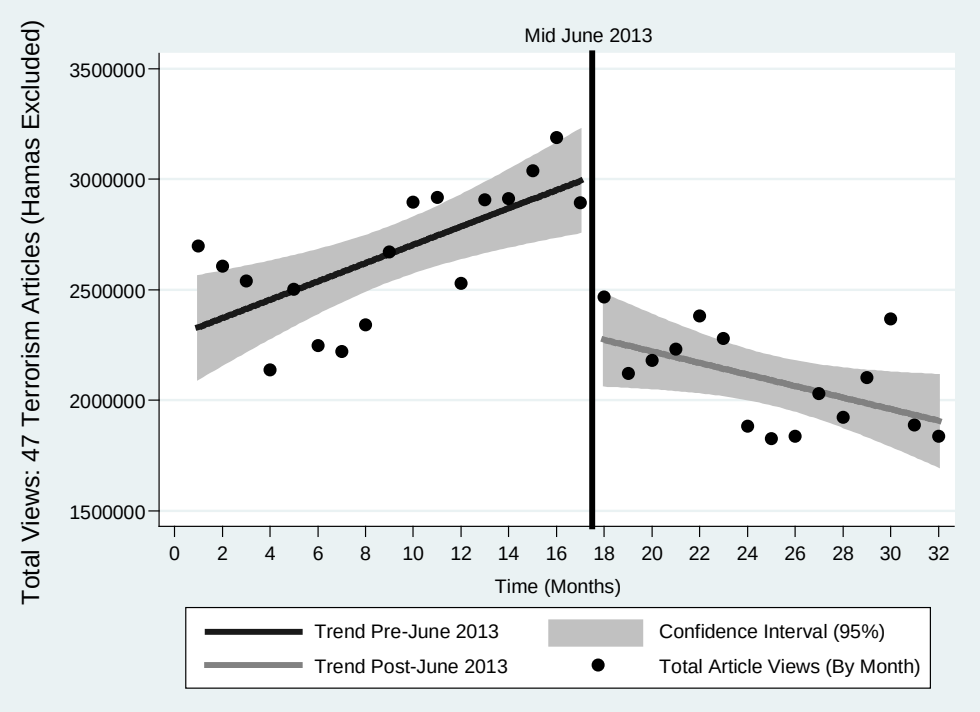


Figure 2. *Pre and Post June 2013 Article View Trends (Outliers Excluded). The sudden drop in views and trend shift—from increasing monthly views over time to decreasing after June 2013—is consistent with a significant and long-term chilling effect.*

45. The shifting trend of the data, which in this case is a sudden and immediate drop, is particularly consistent with a chilling effect arising from the public awareness about NSA surveillance after the June 2013 revelations. If the outlier view count data relating to the Hamas article is excluded, the decline in page views is slightly less substantial (e.g., 23% compared to the 31% drop-off if the Hamas data remains in the study) but in either case, a substantial and statistically significant decrease.

46. Moreover, there is a change in the overall trend in the data. Before June 2013, total views of the Wikipedia articles in the dataset slowly increase each month. After June 2013,

however, with the increased public awareness about NSA surveillance programs, there is a change in the "slope," or data trend. Without the outlier "Hamas" view counts in July 2014, the total views for the Terrorism Wikipedia Articles Group are on a downward path as seen in Figure 2. All of this is consistent with a chilling effect associated with the public awareness about NSA surveillance programs due to June 2013 revelations and reporting—both the reduction in view counts in June 2013 and the overall shift in the monthly article view trend thereafter.

47. The data findings in Table 2 and visualized in Figure 2 offer evidence demonstrating a long-term chilling effect due to the June 2013 surveillance revelations, which is not only associated with an immediate drop in views but also a long-term chill on accessing these Wikipedia articles, as users accessed information on these topics less and less frequently.

iii. Third Set of Results: 31 Most Privacy-Sensitive Wikipedia Terrorism Article Group

48. An additional analysis of the 31 most privacy-concerning Wikipedia articles in the 47 Terrorism Wikipedia Article Group (the articles associated with keywords receiving the highest sensitivity responses in the MTurk survey described in ¶ 33)[38] strengthens the chilling effects hypothesis. Using the 983,860 predicted article views for June 2013 (based on the pre-June monthly view trend), showed an even greater reduction in views in June 2013 of 26% (highly statistically significant at $p<0.01$ level) as well as a highly statistically significant reversal in the overall month to month view counts, due to a reduction of 41,554 monthly views after June 2013. These results, where more privacy-concerning Wikipedia articles lead to an even greater statistically significant view count reduction in June 2013, as well as a likewise reversal in the overall article views on a monthly basis after June 2013, is consistent with a chilling effect

[38] This set includes the 31 terrorism-related articles, among the full-set of 48, that had a combined average privacy rating score above 2 from the MTurk survey—the median score for the set of 48. *See infra* Appendix A, Table 13 ("31 Article Group" list including combined privacy-sensitive score).

hypothesis. Correcting for auto-correlation using the Prais-Winsten method for the 47 Terrorism Wikipedia Article Group did not change these key findings.

49. Further strengthening this chilling effects hypothesis, overall Wikipedia article view traffic trends do not explain these results. Identical analysis of view counts for the English Wikipedia home page (non-mobile platforms data) for the same 32-month period can be found at Table 3 of Appendix. There are clear differences. First, while there is a reduction in views for the English Wikipedia homepage in June 2013, the reduction is significantly less (16% if one considered predicted views for June 2013 based on previous trends). So, even assuming a full 16 percentage points in the total 23% drop off for the 47 terrorism-related Wikipedia articles[39] simply reflects overall English Wikipedia trends, that still leaves 7% of the reduction in article views in June 2013. Similarly, using the 31 most privacy-concerning terrorism-related Wikipedia articles, which as noted above had a 26% reduction in June 2013,[40] would leave a 10% drop unaccounted for by background trends. This is more than twice the noteworthy and statistically significant 4% reduction in Google privacy-sensitive searches that Marthews and Tucker found after June 2013.

50. Moreover, while there is a statistically significant change in monthly article views after June 2013 for the English Wikipedia Homepage, there are again significant differences. The monthly rate of change before June 2013 for the homepage was less than 1 percent of views per month (0.97%) and after June 2013, views reduced on a monthly basis by 0.22%. By stark contrast, the results for the 31 most privacy-concerning Wikipedia Terrorism Articles Group showed that before June 2013, there was a statistically significant monthly increase in views that amounted to a 6% overall increase in article views per month, and after June 2013, monthly views decreased

[39] *See supra* ¶ 43.

[40] *See supra* ¶ 48.

by 2% a month. In other words, the 31 most privacy-concerning article views for these articles were increasing at six times the rate of the English Wikipedia homepage on a monthly basis, and after June 2013 were decreasing monthly at ten times the rate of the English Wikipedia homepage. These differences all suggest that these findings for the 47 Terrorism Wikipedia Articles Group and the 31 most privacy-concerning Terrorism Wikipedia Articles Group reflect more than mere background Wikipedia trends.[41]

51. A further analysis of the 31 most privacy-concerning Terrorism Articles Group, which includes English Wikipedia Homepage views (non-mobile platforms data) as a control (see Table 8), provides even more support. Using the 1,012,950 predicted article views for June 2013, these results also showed a greater reduction in views in June 2013 of 31% (highly statistically significant at $p < 0.01$ level), as well as a highly statistically significant reversal in the overall month-to-month view counts, due to a reduction of 46,226 monthly views after June 2013. An identical analysis of the 47 Terrorism Articles Group, also with English Wikipedia Homepage views as a control (see Table 9), yielded a 20% highly statistically significant reduction in views in June 2013 and a highly statistically reversal in overall month-to-month view, due to a reduction of 60,504 monthly views after June 2013. There was also no correlation found between either the 31 or 47 Terrorism Article Groups and the English Wikipedia Homepage views. These findings are consistent with a chilling effects hypothesis.

iv. Comparator Wikipedia Article Groups

52. The conclusions of this statistical analysis are further strengthened by analyses carried out on three different "comparator" groups of Wikipedia articles. Using the same statistical methods described above, analyses of the comparator groups showed neither a statistically

[41] Marthews & Tucker, *supra* note 4, at 3.

significant reduction in article views in June 2013, nor a shift in the overall trend in article views after that month. These comparator Wikipedia article groups included a group of 25 security-related Wikipedia articles;[42] 34 infrastructure-related Wikipedia articles;[43] and a group of the 26 most popular Wikipedia articles in 2012, 2013, and 2014.[44]

53. As Figure 3 illustrates, unlike the 47 Terrorism Wikipedia Article Group, results from an identical analysis for the group of 25 domestic "security"-related Wikipedia articles showed no statistically significant reduction in article views in June 2013 and no statistically significant change in the trend in the data.

[42] The methodology for selecting Wikipedia articles for the security comparator group was the same as that used for the original 48 Wikipedia Terrorism articles. Wikipedia articles corresponding with keywords set out in the DHS keyword list for domestic security ("DHS & Other Agencies" keyword category) were included. Locating Wikipedia articles coinciding with each keyword was again done manually, and similarly, there was a Wikipedia article that corresponded perfectly with the vast majority of keywords in the "DHS & Other Agencies" keyword category. The 25 Wikipedia articles are included in Appendix A at Table 14.

[43] The methodology for selecting Wikipedia articles for the infrastructure group was the same as for the terrorism and domestic security Wikipedia article groups. Here, Wikipedia articles were selected that corresponded to DHS keywords for the "Infrastructure Security" keyword category. Again, locating articles was straightforward, as there was a Wikipedia article that corresponded naturally with the vast majority of keywords in the "Infrastructure Security" keyword category. All 34 Wikipedia articles are included in Appendix A at Table 15.

[44] The top 10 most popular English Wikipedia articles (in terms of article views) for each of years 2012, 2013, and 2014 (the years included in the 32-month study period) were included in the "popular" Wikipedia article comparator group. This was determined by consulting the Wikimedia Tool Lab's "Wikitrend" reports (https://tools.wmflabs.org/wikitrends), resulting in a set of 26 Wikipedia articles comparator group, including articles like "Google," "Facebook," "Breaking Bad," "Game of Thrones," and "World War II." Certain Wikipedia articles like "Facebook" and "Google" were in the top ten most popular articles for more than one year, hence 26 articles instead of 30. The 26 popular articles group is listed in Appendix A at Table 16.

Figure 3. *The highly statistically significant (at the $p<0.01$ level) substantial view count reduction in June 2013 as well as the shift to fewer monthly article views after June 2013 for the terrorism articles is consistent with a chilling effect. There are no statistically significant findings for the comparator article groups.*

Wikipedia Article Group	Monthly trend pre-June 2013	Change in view count in June 2013	Change in monthly trend after June 2013	Model Fit
47 Terrorism Articles	**41,420.51**** ***p*=0.00**	**−693,616.9**** ***p*=0.00**	**−67,513.1**** ***p*=0.00**	**Yes** ***F*=0.00**
25 Security Articles	11,135.0 $p=0.187$	−24,638.34 $p=0.84$	−20,465.87 $p=0.12$	No $F=0.45$
34 Infrastructure Articles	**−11,079**** ***p*=0.00**	−12,721.0 $p=0.77$	2,431.84 $p=0.61$	**Yes** ***F*=0.00**
26 Popular Articles	−48,458 $p=0.798$	−1,716,643 $p=0.53$	177,324.7 $p=0.551$	No $F=0.79$

Statistically significant findings in bold (*p<0.05, **p<0.01).

54. In fact, the overall model fit for this analysis was not significant, meaning the public awareness about NSA surveillance programs in June 2013 revelations has no value for predicting article views and view trends for these 25 domestic security related articles.[45]

55. The 34 "infrastructure" Wikipedia article comparator group results also showed no statistically significant reduction in article view counts after the June 2013 revelations, nor any statistically significant change in the overall month-to-month trend in the view count data after that month. Correcting for autocorrelation in these results does not change these key observations.

56. Finally, the results for an identical analysis on the 26 "popular" Wikipedia article comparator group likewise showed no statistically significant reduction in views or any monthly

[45] When the F-test or F-value for a regression analysis result is not significant (greater than 0.05) then the analysis (and results) are not reliable and have no predictive value. *See* Karen Grace-Martin, *Assessing the Fit of Regression Models*, THE ANALYSIS FACTOR: MAKING STATISTICS MAKE SENSE (Online), https://www.theanalysisfactor.com/assessing-the-fit-of-regression-models/; MARKO SARSTADT AND ERIK MOOI, A CONCISE GUIDE TO MARKET RESEARCH: THE PROCESS, DATA, AND METHODS USING IBM SPSS STATISTICS 212 (2014).

change in view count trends in relation to June 2013. Like the security comparator groups, the model fit for this analysis was not significant.

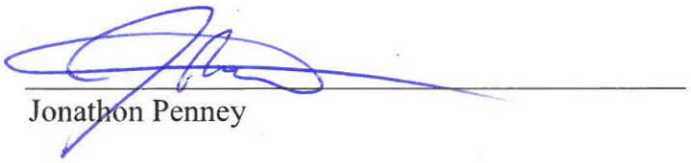
57. These results are all consistent with a chilling effects hypothesis. Unlike the privacy-concerning 47 Terrorism Wikipedia Article Group, the comparator Wikipedia article groups showed no comparable page view reductions in June 2013, nor a change in view count data trends after June 2013. These comparator results strengthen the conclusion that the statistically significant shift in article view counts post-June 2013 for the privacy-concerning Wikipedia articles is attributable to NSA-related chilling effects, and not to other background or confounding variables.

VI. CONCLUSION

58. In sum, I conclude that the highly statistically significant and substantial reduction in view counts in June 2013, as well as the highly statistically significant trend reversal in the monthly article views after June 2013, for both the 47 Terrorism Wikipedia Articles Group and the 31 most privacy-concerning Terrorism Wikipedia Articles Group, offers compelling evidence that increased public awareness about NSA surveillance programs in June 2013 had a chilling effect on Wikipedia users.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Executed on December 18, 2018 in Halifax, Canada.



Jonathon Penney

APPENDIX A

Table 1: First Results, 48 Terrorism-related Articles Study Group

(No autocorrelation concerns with Durbin-Watson Test of 1.50)

Independent Variable	Coefficients	Standard Error	*P*-value
Coefficient (β_0)	**23522364****	171743.1	0.000
Expected Total Views at Beginning of Study			
Pre June 2013 trend in data (β_1)	**47038.28****	16760.41	0.009
Change in Views (Monthly) Before 6/2013			
Change in level (β_2)	**−995085.2***	241987.6	0.000
Change in Views Immediately After 6/2013			
Change in slope (β_3)	−35517.69	26272.41	0.187
Change in Views (Monthly) After 6/2013			

*$p<0.05$, **$p<0.01$

Table 2: Second Results, 47 Terrorism-related Articles (Hamas Excluded)

Durbin-Watson Test Result (1.33)
Results correcting auto-correlation (Prais–Winsten method) in parenthesis

Independent Variable	Coefficients	Standard Error	*P*-value
Coefficient (β_0)	**2289153**** **(2349041.0)**	109751.5 (144474.7)	0.000 (0.000)
Expected Total Views at Beginning of Study			
Pre June 2013 trend in data (β_1)	**41420.51**** **(34813.9)***	10710.65 (13824.52)	0.001 (0.02)
Change in Views (Monthly) Before 6/2013			
Change in level (β_2)	**−693616.9 **** **(−594574.2)****	154640.9 (186174.7)	0.000 (0.00)
Change in Views Immediately After 6/2013			
Change in slope (β_3)	**−67513.1**** **(−65683)****	16789.25 (22514.01)	0.000 (0.00)
Change in Views (Monthly) After 6/2013			

*$p<0.05$, **$p<0.01$

Table 3: Global English Wikipedia Article Views, Non-Mobile (Millions)

(No autocorrelation concerns with Durbin-Watson Test of 1.89)

Independent Variable	Coefficients	Standard Error	*P*-value
Coefficient (β_0)	**7385.11****	204.48	0.000
Expected Total Views at Beginning of Study			
Pre June 2013 trend in data (β_1)	**70.57****	19.95	0.000
Change in Views (Monthly) Before 6/2013			
Change in level (β_2)	**−1397.96****	288.11	0.007
Change in Views Immediately After 6/2013			
Change in slope (β_3)	**−90.97****	31.28	0.000
Change in Views (Monthly) After 6/2013			

*$p<0.05$, **$p<0.01$

Table 4: Full 25 Domestic Security-related Wikipedia Articles Comparator Group

Note: This model's fit was not significant (Prob > F = 0.447)

Independent Variable	Coefficients	Standard Error	*P*-value
Coefficient (β_0)	**708187.3****	84366.66	0.00
Expected Total Views at Beginning of Study			
Pre June 2013 trend in data (β_1)	11135.07	8233.34	0.187
Change in Views (Monthly) Before 6/2013			
Change in level (β_2)	−24638.34	118873.4	0.837
Change in Views Immediately After 6/2013			
Change in slope (β_3)	− 20465.87	12905.99	0.124
Change in Views (Monthly) After 6/2013			

*$p<0.05$, **$p<0.01$

Table 5: 34 Infrastructure Security-related Articles Comparator Group

Durbin-Watson Test Result (1.09)
Results correcting auto-correlation (Prais–Winsten method) in parenthesis

Independent Variable	Coefficients	Standard Error	*P*-value
Coefficient (β_0)	**771772.3****	30948.71	0.000
	(785975.7)**	(42559.45)	(0.000)
Expected Total Views at Beginning of Study			
Pre June 2013 trend in data (β_1)	**−11079.82****	3020.28	0.001
	(−11847.06)**	(4040.79)	(0.007)
Change in Views (Monthly) Before 6/2013			
Change in level (β_2)	−12721.07	43607.01	0.773
	(−20678.15)	(52816.07)	(0.698)
Change in Views Immediately After 6/2013			
Change in slope (β_3)	2431.84	4734.38	0.612
	(3464.15)	(6663.93)	(0.607)
Change in Views (Monthly) After 6/2013			

**p*<0.05, ***p*<0.01

Table 6: 26 Most Popular Wikipedia Articles (2012/2013/2014) Comparator Group

Note: This model's fit was not significant (Prob > F = 0.7938)

Independent Variable	Coefficients	Standard Error	*P*-value
Coefficient (β_0)	**2.58×10^7****	1920624	0.000
Expected Total Views at Beginning of Study			
Pre June 2013 trend in data (β_1)	−48458.14	187433.7	0.798
Change in Views (Monthly) Before 6/2013			
Change in level (β_2)	−1716643	2706177	0.531
Change in Views Immediately After 6/2013			
Change in slope (β_3)	177324.7	293807.6	0.551
Change in Views (Monthly) After 6/2013			

**p*<0.05, ***p*<0.01

Table 7: 31 Terrorism-related Wikipedia Articles Study Group

No autocorrelation concerns with Durbin-Watson Test of 1.52

Independent Variable	Coefficients	Standard Error	*P*-value
Coefficient (β_0)	**471146.3****	45966.52	0.000
Expected Total Views at Beginning of Study			
Pre June 2013 trend in data (β_1)	**28484.1****	4485.87	0.000
Change in Views (Monthly) Before 6/2013			
Change in level (β_2)	**−253556.5****	64767.24	0.000
Change in Views Immediately After 6/2013			
Change in slope (β_3)	**−41554.21****	7031.73	0.000
Change in Views (Monthly) After 6/2013			

*$p<0.05$, **$p<0.01$

Table 8: 31 Terrorism-related Wikipedia Articles Study Group (with Control)

Results Controlling For English Wikipedia Homepage Views (Raw, Non-Mobile)
No autocorrelation concerns with Durbin-Watson Test of 1.62

Independent Variable	Coefficients	Standard Error	*P*-value
Coefficient (β_0)	**850386.4***	314365.4	0.01
Expected Total Views at Beginning of Study			
Pre June 2013 trend in data (β_1)	**32108.35****	5349.31	0.000
Change in Views (Monthly) Before 6/2013			
Change in level (β_2)	**− 325345****	87120.19	0.000
Change in Views Immediately After 6/2013			
Change in slope (β_3)	**−46226.01 ****	7955.04	0.000
Change in Views (Monthly) After 6/2013			
Global English Wikipedia Views Control	−51.35	42.11	0.233
Correlation with English Wikipedia Homepage Views (Non-mobile; in millions)			

*$p<0.05$, **$p<0.01$

Table 9: 47 Terrorism-related Wikipedia Articles Study Group (with Control)

Results Controlling For English Wikipedia Homepage Views (Raw, Non-Mobile)
Durbin-Watson Test Result (1.29)
Results correcting auto-correlation (Prais–Winsten method) in parenthesis

Independent Variable	Coefficients	Standard Error	*P*-value
Coefficient (β_0)	**1720195 ***	762994.1	0.03
	(1657787*)	(715964.1)	(0.03)
Expected Total Views at Beginning of Study			
Pre June 2013 trend in data (β_1)	**35983.25 ***	12983.28	0.01
	(29381.58)	(14928.98)	0.05
Change in Views (Monthly) Before 6/2013			
Change in level (β_2)	**−585915.8***	211448.8	0.01
	(−490610*)	(212517.7)	0.03
Change in Views Immediately After 6/2013			
Change in slope (β_3)	**− 60504.2****	19307.63	0.00
	(−56997.38*)	(24479.42)	0.03
Change in Views (Monthly) After 6/2013			
Global English Wikipedia Views Control	77.04	102.22	0.46
	(92.61)	(93.44)	(0.33)
Correlation with English Wikipedia Homepage Views (Non-mobile; in millions)			

*$p<0.05$, **$p<0.01$

Table 10: Independent Rating Results of 415 Internet Users

Rating Type	Mean Rating
Government Trouble Rating	1.95
Privacy-Sensitive Rating	2.01
Browser History Delete Rating	2.00
Avoidance Rating	2.62

Table 11: 48 Terrorism Article Group List

Topic Keywords	Wikipedia Articles
Al Qaeda	https://en.wikipedia.org/wiki/Al-Qaeda
terrorism	https://en.wikipedia.org/wiki/terrorism
terror	https://en.wikipedia.org/wiki/terror
attack	https://en.wikipedia.org/wiki/attack
Iraq	https://en.wikipedia.org/wiki/iraq
Afghanistan	https://en.wikipedia.org/wiki/afghanistan
Iran	https://en.wikipedia.org/wiki/iran
Pakistan	https://en.wikipedia.org/wiki/pakistan
agro	https://en.wikipedia.org/wiki/agro
Environmental terrorism	https://en.wikipedia.org/wiki/Environmental_terrorism
Eco terrorism	https://en.wikipedia.org/wiki/Eco-terrorism
Conventional weapon	https://en.wikipedia.org/wiki/Conventional_weapon
Weapons grade	https://en.wikipedia.org/wiki/Weapons-grade
dirty bomb	https://en.wikipedia.org/wiki/Dirty_bomb
Nuclear Enrichment	https://en.wikipedia.org/wiki/Nuclear_enrichment
Nuclear	https://en.wikipedia.org/wiki/nuclear
Chemical weapon	https://en.wikipedia.org/wiki/Chemical_weapon
Biological weapon	https://en.wikipedia.org/wiki/Biological_weapon
Ammonium nitrate	https://en.wikipedia.org/wiki/Ammonium_nitrate
Improvised explosive device	https://en.wikipedia.org/wiki/Improvised_explosive_device
Abu Sayyaf	https://en.wikipedia.org/wiki/Abu_Sayyaf
Hamas	https://en.wikipedia.org/wiki/hamas
FARC	https://en.wikipedia.org/wiki/FARC
Irish Republican Army	https://en.wikipedia.org/wiki/Irish_Republican_Army
Euskadi ta Askatasuna	https://en.wikipedia.org/w/Euskadi_ta_Askatasuna
Hezbollah	https://en.wikipedia.org/wiki/hezbollah
Tamil Tigers	https://en.wikipedia.org/wiki/Tamil_Tigers
PLO	https://en.wikipedia.org/wiki/Palestine_Liberation_Organization
Palestine Liberation Front	https://en.wikipedia.org/wiki/Palestine_Liberation_Front
Car bomb	https://en.wikipedia.org/wiki/Car_bomb
jihad	https://en.wikipedia.org/wiki/jihad
Taliban	https://en.wikipedia.org/wiki/taliban
Suicide bomber	https://en.wikipedia.org/wiki/Suicide_bomber
Suicide attack	https://en.wikipedia.org/wiki/Suicide_attack
AL Qaeda in the Arabian Peninsula	https://en.wikipedia.org/wiki/Al-Qaeda_in_the_Arabian_Peninsula
Al Qaeda in the Islamic Maghreb	https://en.wikipedia.org/wiki/Al-Qaeda_in_the_Islamic_Maghreb
Tehrik-i-Taliban Pakistan	https://en.wikipedia.org/wiki/Tehrik-i-Taliban_Pakistan
Yemen	https://en.wikipedia.org/wiki/yemen
Pirates	https://en.wikipedia.org/wiki/pirates
Extremism	https://en.wikipedia.org/wiki/extremism

Somalia	https://en.wikipedia.org/wiki/somalia
Nigeria	https://en.wikipedia.org/wiki/nigeria
Political radicalism	https://en.wikipedia.org/wiki/Political_radicalism
Al-Shabaab	https://en.wikipedia.org/wiki/Al-Shabaab
nationalism	https://en.wikipedia.org/wiki/nationalism
Recruitment	https://en.wikipedia.org/wiki/recruitment
Fundamentalism	https://en.wikipedia.org/wiki/fundamentalism
Islamist	https://en.wikipedia.org/wiki/islamist

Table 12: 48 Terrorism Article Group List with Privacy Survey Scores

Topic Keywords	Government Trouble	Browser Delete	Privacy Sensitive	Avoidance
Al Qaeda	2.20	2.11	2.21	2.84
terrorism	2.19	2.05	2.16	2.79
terror	1.98	1.96	2.01	2.64
attack	1.92	1.91	1.92	2.56
Iraq	1.60	1.74	1.76	2.25
Afghanistan	1.61	1.71	1.75	2.23
Iran	1.62	1.73	1.78	2.25
Pakistan	1.59	1.71	1.75	2.22
agro	1.51	1.80	1.76	2.29
Environmental terrorism	2.20	2.20	2.24	2.92
Eco terrorism	2.22	2.20	2.22	2.92
Conventional weapon	2.03	2.16	2.07	2.81
Weapons grade	2.18	2.22	2.17	2.99
dirty bomb	2.72	2.55	2.50	3.45
Nuclear Enrichment	2.22	2.21	2.21	2.92
Nuclear	1.84	1.97	1.91	2.55
Chemical weapon	2.43	2.36	2.39	3.16
Biological weapon	2.44	2.39	2.39	3.18
Ammonium nitrate	2.49	2.44	2.26	3.24
Improvised explosive device	2.82	2.64	2.53	3.46
Abu Sayyaf	2.02	1.96	1.99	2.57
Hamas	1.90	1.93	1.97	2.49
FARC	1.83	1.88	1.90	2.46
Irish Republican Army	1.62	1.77	1.83	2.24
Euskadi ta Askatasuna	1.86	1.88	1.88	2.43
Hezbollah	1.86	1.90	1.96	2.46
Tamil Tigers	1.76	1.86	1.87	2.39
PLO	1.77	1.87	1.91	2.42
Palestine Liberation Front	1.81	1.89	1.95	2.47
Car bomb	2.72	2.61	2.50	3.40
jihad	2.15	2.19	2.17	2.89
Taliban	2.06	2.03	2.10	2.70
Suicide bomber	2.25	2.31	2.24	2.97
Suicide attack	2.30	2.36	2.29	3.04
AL Qaeda in the Arabian Peninsula	2.01	1.98	2.06	2.63
Al Qaeda in the Islamic Maghreb	2.05	1.98	2.06	2.60
Tehrik-i-Taliban Pakistan	1.96	1.96	1.97	2.59
Yemen	1.60	1.72	1.74	2.18
Pirates	1.44	1.67	1.67	2.10
Extremism	1.64	1.90	1.86	2.40

Somalia	1.50	1.68	1.67	2.12
Nigeria	1.48	1.66	1.64	2.07
Political radicalism	1.75	1.91	1.97	2.48
Al-Shabaab	1.84	1.89	1.89	2.48
nationalism	1.48	1.71	1.73	2.20
Recruitment	1.74	1.90	1.87	2.54
Fundamentalism	1.60	1.79	1.80	2.32
Islamist	1.79	1.89	1.93	2.45
MEAN	**1.95**	**2.00**	**2.01**	**2.62**

Table 13: 31 Most Privacy-Concerning Terrorism Article Group (survey privacy-rating above 2)

Topic Keywords	Wikipedia Articles	Combined Privacy Rating
Al Qaeda	http://en.wikipedia.org/wiki/Al-Qaeda	2.34
terrorism	http://en.wikipedia.org/wiki/terrorism	2.30
terror	http://en.wikipedia.org/wiki/terror	2.15
Environmental terrorism	http://en.wikipedia.org/wiki/Environmental_terrorism	2.39
Eco terrorism	http://en.wikipedia.org/wiki/Eco-terrorism	2.39
Conventional weapon	http://en.wikipedia.org/wiki/Conventional_weapon	2.27
Weapons grade	http://en.wikipedia.org/wiki/Weapons-grade	2.39
dirty bomb	http://en.wikipedia.org/wiki/Dirty_bomb	2.81
Nuclear Enrichment	http://en.wikipedia.org/wiki/Nuclear_enrichment	2.39
Nuclear	http://en.wikipedia.org/wiki/nuclear	2.07
Chemical weapon	http://en.wikipedia.org/wiki/Chemical_weapon	2.59
Biological weapon	http://en.wikipedia.org/wiki/Biological_weapon	2.60
Ammonium nitrate	https://en.wikipedia.org/wiki/Ammonium_nitrate	2.61
Improvised explosive device	http://en.wikipedia.org/wiki/Improvised_explosive_device	2.86
Abu Sayyaf	http://en.wikipedia.org/wiki/Abu_Sayyaf	2.14
FARC	http://en.wikipedia.org/wiki/FARC	2.02
Euskadi ta Askatasuna	http://en.wikipedia.org/w/Euskadi_ta_Askatasuna	2.01
Hezbollah	http://en.wikipedia.org/wiki/hezbollah	2.05
Palestine Liberation Front	http://en.wikipedia.org/wiki/Palestine_Liberation_Front	2.03
Car bomb	http://en.wikipedia.org/wiki/Car_bomb	2.81
jihad	http://en.wikipedia.org/wiki/jihad	2.35
Taliban	http://en.wikipedia.org/wiki/taliban	2.22
Suicide bomber	http://en.wikipedia.org/wiki/Suicide_bomber	2.44
Suicide attack	http://en.wikipedia.org/wiki/Suicide_attack	2.50
AL Qaeda in the Arabian Peninsula	http://en.wikipedia.org/wiki/Al-Qaeda_in_the_Arabian_Peninsula	2.17
Al Qaeda in the Islamic Maghreb	http://en.wikipedia.org/wiki/Al-Qaeda_in_the_Islamic_Maghreb	2.17
Tehrik-i-Taliban Pakistan	http://en.wikipedia.org/wiki/Tehrik-i-Taliban_Pakistan	2.12
Political radicalism	http://en.wikipedia.org/wiki/Political_radicalism	2.03
Al-Shabaab	http://en.wikipedia.org/wiki/Al-Shabaab	2.03
Recruitment	http://en.wikipedia.org/wiki/recruitment	2.01
Islamist	http://en.wikipedia.org/wiki/islamist	2.02

Table 14: 25 Domestic Security Article List

Topic Keywords	Wikipedia Articles
Department of Homeland Security	https://en.wikipedia.org/wiki/United_States_Department_of_Homeland_Security
Federal Emergency Management Agency	https://en.wikipedia.org/wiki/Federal_Emergency_Management_Agency
Coast Guard	https://en.wikipedia.org/wiki/Coast_guard
Customs and Border Protection	https://en.wikipedia.org/wiki/Customs_and_Border_Protection
Border patrol	https://en.wikipedia.org/wiki/Border_Patrol
Secret Service	https://en.wikipedia.org/wiki/Secret_Service
Bureau of Land Management	https://en.wikipedia.org/wiki/Bureau_of_Land_Management
Homeland defense	https://en.wikipedia.org/wiki/Homeland_defense
Agent / Espionage	https://en.wikipedia.org/wiki/Espionage
Task Force 88	https://en.wikipedia.org/wiki/Task_Force_88_(anti-terrorist_unit)
Central Intelligence Agency	https://en.wikipedia.org/wiki/Central_Intelligence_Agency
Fusion center	https://en.wikipedia.org/wiki/Fusion_center
DEA	https://en.wikipedia.org/wiki/DEA
Secure Border Initiative	https://en.wikipedia.org/wiki/Secure_Border_Initiative
Federal Bureau of Investigation	https://en.wikipedia.org/wiki/Federal_Bureau_of_Investigation
Alcohol and Tobacco Tax and Trade Bureau	https://en.wikipedia.org/wiki/Alcohol_and_Tobacco_Tax_and_Trade_Bureau
U.S. Citizenship and Immigration Services	https://en.wikipedia.org/wiki/United_States_Citizenship_and_Immigration_Services
Federal Air Marshal Service	https://en.wikipedia.org/wiki/Federal_Air_Marshal_Service
Transportation Security Administration	https://en.wikipedia.org/wiki/Transportation_Security_Administration
Air Marshal	https://en.wikipedia.org/wiki/Air_marshal
Federal Aviation Administration	https://en.wikipedia.org/wiki/Federal_Aviation_Administration
National Guard	https://en.wikipedia.org/wiki/National_Guard
Disaster Relief / Emergency Management	https://en.wikipedia.org/wiki/Emergency_management
U.S. Immigration and Customs Enforcement	https://en.wikipedia.org/wiki/U.S._Immigration_and_Customs_Enforcement
United Nations	https://en.wikipedia.org/wiki/United_Nations

Table 15: 34 Infrastructure Article List

Topic Keywords	Wikipedia Articles
Information security	https://en.wikipedia.org/wiki/Infrastructure_security
Airport	https://en.wikipedia.org/wiki/Airport
Airplane	https://en.wikipedia.org/wiki/Airplane
Chemical burn	https://en.wikipedia.org/wiki/Chemical_burn
CIKR	https://en.wikipedia.org/wiki/CIKR
AMTRAK	https://en.wikipedia.org/wiki/Amtrak
Collapse	https://en.wikipedia.org/wiki/Collapse
Information infrastructure	https://en.wikipedia.org/wiki/Information_infrastructure
Telecommunications network	https://en.wikipedia.org/wiki/Telecommunications_network
Telecommunication	https://en.wikipedia.org/wiki/Telecommunication
Critical infrastructure	https://en.wikipedia.org/wiki/Critical_Infrastructure
National Information Infrastructure	https://en.wikipedia.org/wiki/National_Information_Infrastructure
Metro	https://en.wikipedia.org/wiki/Metro_station
WMATA	https://en.wikipedia.org/wiki/Washington_Metropolitan_Area_Transit_Authority
Subway	https://en.wikipedia.org/wiki/Subway
BART	https://en.wikipedia.org/wiki/Bay_Area_Rapid_Transit
MARTA	https://en.wikipedia.org/wiki/Metropolitan_Atlanta_Rapid_Transit_Authority
Port authority	https://en.wikipedia.org/wiki/Port_authority
NBIC	https://en.wikipedia.org/wiki/NBIC
Power grid	https://en.wikipedia.org/wiki/Electrical_grid
Power	https://en.wikipedia.org/wiki/Power
Smart	https://en.wikipedia.org/wiki/Smart
Full body scanner	https://en.wikipedia.org/wiki/Full_body_scanner
Electric power	https://en.wikipedia.org/wiki/Electric_power
Failure	https://en.wikipedia.org/wiki/Failure
Power outage	https://en.wikipedia.org/wiki/Power_outage
Blackout	https://en.wikipedia.org/wiki/Blackout
Brownout	https://en.wikipedia.org/wiki/Brownout
Port	https://en.wikipedia.org/wiki/Port
Dock (maritime)	https://en.wikipedia.org/wiki/Dock_(maritime)
Bridge	https://en.wikipedia.org/wiki/Bridge
Flight cancellation and delay	https://en.wikipedia.org/wiki/Flight_cancellation_and_delay
Delay	https://en.wikipedia.org/wiki/Delay
Electric power transmission	https://en.wikipedia.org/wiki/Electric_power_transmission

Table 16: 26 Most Popular Articles in 2012, 2013, and 2014 Comparator Group

Topic Keywords	Wikipedia Articles
Facebook	https://en.wikipedia.org/wiki/Facebook
Wiki	http://en.wikipedia.org/wiki/Wiki
Deaths in 2012	https://en.wikipedia.org/wiki/Lists_of_deaths_by_year#2012
One Direction	https://en.wikipedia.org/wiki/One_Direction
The Avengers (2012 film)	https://en.wikipedia.org/wiki/The_Avengers_(2012_film)
Fifty Shades of Grey	https://en.wikipedia.org/wiki/Fifty_Shades_of_Grey
2012 phenomena	https://en.wikipedia.org/wiki/2012_phenomenon
Google	https://en.wikipedia.org/wiki/Google
The Dark Knight Rises	https://en.wikipedia.org/wiki/The_Dark_Knight_Rises
The Hunger Games	https://en.wikipedia.org/wiki/The_Hunger_Games
Deaths in 2013	https://en.wikipedia.org/wiki/Lists_of_deaths_by_year#2013
Breaking Bad	https://en.wikipedia.org/wiki/Breaking_Bad
G-force	https://en.wikipedia.org/wiki/G-force
World War II	https://en.wikipedia.org/wiki/World_War_II
Youtube	https://en.wikipedia.org/wiki/YouTube
List of Bollywood Films 2013	https://en.wikipedia.org/wiki/List_of_Bollywood_films_of_2013
United States	https://en.wikipedia.org/wiki/United_States
Online shopping	https://en.wikipedia.org/wiki/Online_shopping
Java	https://en.wikipedia.org/wiki/Java
Alive	https://en.wikipedia.org/wiki/Alive
Deaths in 2014	https://en.wikipedia.org/wiki/Lists_of_deaths_by_year#2014
Climatic Research Unit email controversy	https://en.wikipedia.org/wiki/Climatic_Research_Unit_email_controversy
Amazon.com	https://en.wikipedia.org/wiki/Amazon.com
2014 FIFA World Cup	https://en.wikipedia.org/wiki/2014_FIFA_World_Cup
Ebola virus disease	https://en.wikipedia.org/wiki/Ebola_virus_disease
Game of Thrones	https://en.wikipedia.org/wiki/Game_of_Thrones

Appendix B

JONATHON W. PENNEY

Schulich School of Law, Dalhousie University
6061 University Ave, Halifax, NS, Canada, B3A 4M6
Phone: +(902) 830 3008 // Email: jon@dal.ca
Website: https://jonpenney.com

Dr. Jonathon Penney is a lawyer and social scientist who does research at the intersection of law, technology, and human rights. From the internet today to artificial intelligence and beyond tomorrow, his work aims to understand technology's role in public and private sector censorship, surveillance, and other emerging legal/regulatory practices. He has held appointments at the leading research centers in his field, including the Oxford Internet Institute, University of Oxford; Harvard's Berkman Klein Center for Internet and Society; Princeton's Center for Information Technology Policy; and the Massachusetts Institute of Technology's Media Lab. He is also the author of numerous publications and is a frequent speaker at technology law and policy conferences around the world.

Dr. Penney has studied law at Columbia Law School as a Fulbright Scholar and at Oxford as a Mackenzie King Scholar. He holds a doctorate in "Information, Communication, and the Social Sciences" from the interdisciplinary Oxford Internet Institute at the University of Oxford.

He has a particular expertise in measuring and exploring the impact of surveillance and other data driven and technology-focused regulatory activities, and is author of the book *Chilling Effects: Understanding the Impact of Surveillance and Other Technological Threats* (forthcoming in Cambridge University Press, 2019). His work has received international attention and coverage, including the *Washington Post*, *Reuters International*, *New York Times*, *Newsweek*, *TIME Magazine*, *NBC News*, *Forbes*, *Psychology Today*, *Le Monde*, *The Guardian*, *Freitag*, *Il Fatto Quotidiano*, *The Times of India*, *Indian Express*, *Jerusalem Post*, *Huffington Post*, *Politico*, *Slate*, *Motherboard*, *The Hill*, *The Index on Censorship*, as well as coverage by Pulitzer Prize winning journalist Glenn Greenwald in *The Intercept*.

CURRENT APPOINTMENTS / AFFILIATIONS

Schulich School of Law, Dalhousie University
Associate Professor, July 2018 – Present
Director, *Law and Technology Institute*, September 2017 – Present

Center for Information Technology Policy, Princeton University
Research Affiliate, September 2017 – Present

MIT Media Lab, Massachusetts Institute of Technology
Research Associate (Civil Servant Project), January 2018 – Present

Citizen Lab, Munk School of Global Affairs, University of Toronto
Research Fellow, September 2017 – Present

EDUCATION

Oxford Internet Institute, University of Oxford (Balliol College)
DPhil, Doctorate in Information, Communication, and the Social Sciences, January 2016
Thesis: Chilling Effects in the Internet Age: Three Case Studies
Committee: Dr. Victoria Nash (Oxford), Dr. Urs Gasser (Harvard), Dr. Joss Wright (Oxford)
Google Policy Fellow; SSHRC Doctoral Fellow; Centennial Scholar

Columbia Law School, Columbia University
LLM, Master of Laws, May 2009 (Harlan Fiske Stone Scholar; Fulbright Scholar; GLS Scholar)

Faculty of Law, University of Oxford (Wolfson College)
MSt, Master of Studies (Law), July 2007 (Lady Margaret Hall Award; Mackenzie King Scholar)
Associate-Editor, Oxford University Commonwealth Law Journal

Schulich School of Law, Dalhousie University
JD, Juris Doctorate, May 2003 (Dean's List; Tom Wilcox Award)
Editor of Reviews, Dalhousie Journal of Legal Studies

Faculty of Arts and Social Sciences, Dalhousie University
BA, Philosophy with minor Computer Science credits, May 2000 (Dean's List)

PAST APPOINTMENTS / EMPLOYMENT

Berkman Klein Center for Internet & Society, Harvard University
Berkman Fellow/Research Affiliate, September 2012 – September 2015

Citizen Lab, Munk School of Global Affairs, University of Toronto
Google Policy Fellow, May 2011 – September 2011

PVNets Project, Oxford Internet Institute, University of Oxford
Project Coordinator, September 2010 – September 2012

Faculty of Law, Victoria University of Wellington, Wellington, NZ
InternetNZ Cyberlaw Senior Research Fellow, September 2009 – September 2010

Regulatory Division, Ontario Regional Office, Department of Justice, Toronto
Litigation Counsel, September 2004 – September 2008

PUBLICATIONS

Books

"Chilling Effects: Understanding the Impact of Surveillance and Other Technological Threats" Cambridge University Press, forthcoming 2019

Articles

"The Expressive Value of Cyber-Stalking Laws" (2019) Fordham Law Review ____, forthcoming (with Danielle Citron)

"Privacy, Chilling Effects, and Personalized Legal Automation: The DMCA as an Empirical Case Study" (2019) Stanford Technology Law Review____

"Chilling Effects and the GDPR" (2019) European Law Journal ___, forthcoming (**peer reviewed**)

"Advancing Human Rights-by-Design in the Dual-Use Technology Industry" (with Lex Gill, Sarah McKune, and Ron Deibert), (2019) Columbia Journal of International Affairs, forthcoming (**peer reviewed**)

"Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study", (2017) 6(2) Internet Policy Review 1 (**peer reviewed**)

- Invited to write op-ed discussing paper's findings for *Slate*; research has also received coverage from *WIRED Magazine*, *Global Voices' Netizen Report*, *Slate France*, *Business Insider*, *Privacy Weekly*, European Digital Rights' *EDRi-Gram Report*, and Columbia University's *The Education Lab*.
- Top ten most downloaded article in July 2017 for multiple Social Science Research Network (SSRN) subject areas, incl. "Cyberspace Law", "Information Privacy Law" and "National Security Law".

"Chilling Effects: Online Surveillance and Wikipedia Use", (2016) 31 Berkeley Technology Law Journal 117

- Received extensive media coverage internationally, including the *Washington Post*, *New York Times*, *Newsweek*, *Reuters*, *NBC News*, *Forbes*, *Huffington Post*, *Le Monde*, *Der Freitag*, *Times of India*, *Jerusalem Post*, *Russia Today*, *Daily Mail*, *ABC News Australia*, *The Pakistan Express Tribune*, etc, as well as coverage by Pulitzer Prize winning journalist Glenn Greenwald in *The Intercept*
- #1 most downloaded article on SSRN in the week of May 13th, 2016 and the #2 most downloaded in the week of May 6, 2016; #66 most downloaded in last 12 months

"The Cycles of Global Telecommunication Censorship and Surveillance", (2015) 35 University of Pennsylvania Journal of International Law 693

"Virtual Inequality: Challenges for the Net's Lost Founding Value", (2012) 10 Northwestern Journal of Technology & Intellectual Property 209

"Open Connectivity, Open Data: Two Dimensions of the Right to Seek, Receive, and Impart Information", (2012) 4 Victoria University of Wellington Law Review 1 (**peer reviewed)**

"Internet Access Rights: A Brief History and Intellectual Origins" (2011) 38 William Mitchell Law Review 10 (**invited contribution**)

"Ivan Rand's Ancient Constitutionalism" (2010) 61 UNB Law Journal 43; (2010) 34 Manitoba Law Journal 43 (**peer reviewed)**

- This article won the **2011 Peter Oliver Prize in Canadian Legal History** (for "best article"), Osgoode Society for Canadian Legal History, Law Society of Upper Canada

"Technology and Judicial Reason: Digital Copyright, Secondary Liability, and the Problem of Perspective" (2010) 22 Journal of Intellectual Property 253 (2010) (**peer reviewed**)

"Understanding the New Virtualist Paradigm" (2009) 12 Journal of Internet Law 6

"Privacy and the New Virtualism" (2008) 10 Yale Journal of Law & Technology 194

"The Embarrassing Preamble? Understanding the 'supremacy of God' and the Charter" (2006) 39:2

University of British Columbia Law Review (with Robert Danay) 287 (**peer reviewed**)

"Deciding in the Heat of the Constitutional Moment: Constitutional Meaning and Change in the Quebec Secession Reference" (2005) 28:1 Dalhousie Law Journal 217 (**peer reviewed**)

"The Evolving Approach to Section 15(1): Diminished Rights or Bolder Communities?" (2005) 29 SUPREME COURT LAW REVIEW (2d) 137 (presented at the 8th Annual Constitutional Cases Conference at Osgoode Hall Law School, April 2005) (**peer reviewed**)

A Constitution for the Disabled or a Disabled Constitution? Toward a New Approach to Disability for the Purposes of Section 15(1)" (2003) 1 Journal of Law & Equality 83 (**peer reviewed**)

- Supporting document for World Health Organization and Pan-American Health Organization's 2004 International Convention on Intellectual Disabilities

Book Chapters / Contributions to Collective Works

"Cyber Security, Empiricism, and Human Rights: The Case of State and Non-State Surveillance" in Paul Cornish (eds), Oxford Handbook on Cyber Security (Oxford University Press, forthcoming 2019) (**peer reviewed**)

"Canadian Privacy Law and the Post War Freedom of Information Paradigm" in Gloria González Fuster, Rosamunde van Brakel and Paul De Hert (eds, Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics (Edgar, forthcoming 2018) (**peer reviewed**)

"*Zeran v AOL*'s Chilling Effect Claims" in Eric Goldman, ed, *Zeran v America Online 20 Years Later: A Compendium* (forthcoming 2018)

"Trade Secrets as Intellectual Property: Three Questions," in Mistrale Goudreau, Margaret Ann Wilkinson, & Florian Martin-Bariteau, eds, *New Paradigms in the Protection of Inventiveness, Data and Signs: Changing Perceptions of the Role of Intellectual Property* (Toronto: Irwin Law, forthcoming 2018) (**peer reviewed)**

Copyright's Media Theory and the Internet: The Case of the Chilling Effects Doctrine," in Courtney B Doagoo, Mistrale Goudreau, Madelaine Saginur & Teresa Scassa, eds, *Intellectual Property for the 21st Century: Interdisciplinary Perspectives on Intellectual Property Law* (Toronto: Irwin Law, 2013) (R) (**peer reviewed)**

Essays / Reports / Working papers

"Planet Netsweeper", Citizen Lab Research Report No. 2018-3, Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto, 2018

- This report documented how a Canadian company Netsweeper's web filtering technology has been used by oppressive governments around the world to facilitate censorship and other human rights abuses around the world received widespread media attention in Canada, including a special feature coverage on *CBC's The National*, the broadcaster's flagship national news program.

"Children and Cyberwar: Victimization and Protection" in Dustin Johnson, ed, *Allons-Y: Theory Into Action*, vol 2 (Halifax: The Roméo Dallaire Child Soldiers Initiative, August 2017).

"Can Cyber-Harassment Laws Encourage Online Speech?" in *Harmful Speech Online: At the Intersection of Algorithms and Human Behavior*, Berkman Klein Center Research Publication/Report, Berkman Klein Center for Internet & Society, Harvard University, 2017

"Chilling Effects and the DMCA: Comments in Response to Notice of Inquiry", submission to the U.S. Copyright Office for its Study of Section 512 of Title 17, United States Code (the Digital Millennium Copyright Act), March 30, 2016

"Warrant Canaries Beyond the First Amendment" in *Internet Monitor 2014*: *Reflections on the Digital World: Platforms, Policy, Privacy, and Public Discourse*, Berkman Klein Center Research Publication/Report, Berkman Klein Center for Internet & Society, Harvard University, 2014

"Code is Law, But Law is Increasingly Determining the Ethics of Code" in *Internet Monitor 2014: Reflections on the Digital World: Platforms, Policy, Privacy, and Public Discourse*, Berkman Klein Center Research Publication/Report, Berkman Klein Center for Internet & Society, Harvard University, 2014

"Communications Disruption and Censorship Under International Law", Free and Open Communications on the Internet (FOCI) Working Paper No. 9, USENIX Security Symposium, Advanced Computing Systems Association (ACSA), Bellevue, Washington, 2012 (**peer reviewed**)

Doctoral Thesis

"Chilling Effects in the Internet Age: Three Case Studies" (DPhil Thesis, University of Oxford, November 2015 [unpublished]) (**peer reviewed**)

- Successfully defended in November, 2015 with with no corrections, confirmed December 2016, and degree officially awarded in May 2018.

Public Policy / Commentary / Op-Eds

"How Surveillance Contributes to Fake News", Freedom to Tinker Blog, Center for Information Technology Policy, Princeton University, November, 2018 (forthcoming)

"(Mis)Conceptions about the Impact of Surveillance", Freedom to Tinker Blog, Center for Information Technology Policy, Princeton University, February 14, 2018

"Whose Speech Is Chilled by Surveillance?" Slate Magazine (Online), July 11, 2017

"How Surveillance Harms", Policy Options (Blog), December 12, 2016, Institute for Research on Public Policy (IRPP), Montreal, QC

"How can Atlantic Canada benefit from CETA?", Policy Options (Blog), October 25, 2016, Institute for Research on Public Policy (IRPP), Montreal, QC

"Harper's Charter Activism.", Policy Options (Blog), March 13, 2016, Institute for Research on Public Policy (IRPP), Montreal, QC

"An Amended Bill C-51 is Still a Problem: Lessons from the U.S.", Policy Options Magazine (May-June, 2015), Institute for Research on Public Policy (IRPP), Montreal, QC

"How Laws Are Increasingly Determining the Ethics of Code", Slate Magazine, January 9, 2015

"Constitutional Dialogue v2.0? Contentious Government Responses to the Supreme Court of Canada" (August 2014) Int'l J Const L Blog

"Doomed to Rely on the Mask", Policy Options Magazine , May-June, 2014) Institute for Research on Public Policy (IRPP), Montreal, QC

"Forget CSIS: It's the Political Parties that Own Our Privacy", Toronto Star, March 17, 2014

"Fighting Surveillance: What Canadian Companies Can Do" Citizen Lab (Blog), Munk School of Global Affairs, University of Toronto, February 13, 2014

"Deleting Revenge Porn", Policy Options Magazine , (Nov-Dec 2013), Institute for Research on Public Policy (IRPP), Montreal, QC

"Watching the Watchers: A Role for the ITU in the Internet Age", Cyberdialogue Blog, March 5, 2013, University of Toronto (**invited contribution)**

"Outsourcing Cyberwar", *The Future of Fighting and How the Canadian Military Must Adapt: Strategic Studies Working Group*, Canadian International Council & Canadian Defence and Foreign Affairs Institute, May 25, 2012 (**invited contribution**)

"Time to Get Serious About Cyber-Security", The Mark News (28 July 2011); Information Warfare Monitor, Citizen Lab, Munk School of Global Affairs, University of Toronto (July 2011)

"Countering the Anti-Counterfeiting Trade Agreement", Computer World, November 27, 2009

PRESENTATIONS / TALKS / INVITED LECTURES

Featured Speaker, "The First Amendment and Modern Surveillance", co-hosted by Yale Law School Information Society Project and Knight First Amendment Institute, Columbia University, November 14, 2018 (**invited**)

"Geneva Dialogue On Responsible Behaviour in Cyberspace ", Swiss Federal Department of Foreign Affairs, Geneva, Switzerland, November 1-2, 2018 (**invited**)

Session Discussant, "AI in Criminal Justice", DeepMind / Princeton CITP Limits of AI in Public Service Workshop, Center for Information Technology Policy, Princeton University, September 28, 2018 (**invited**)

"Measuring the Impact of Surveillance and Other Online Threats at Scale", The Emergence of Computational Legal Studies: The Promises and Challenges of Data-Driven Legal Research, First Annual Computational Legal Studies Workshop, Department of Law / Law and Technology Centre, University of Hong Kong, Hong Kong, June 28-29, 2018 (**invited**)

"Internet Surveillance: An Empirical and Comparative Case Study", 11th Annual Privacy Law Scholars Conference, George Washington University Law Center, Washington DC, May 30-31 2018 (**invited**)

Featured Speaker, RightsCon Summit (Toronto), May 16-18 2018, Toronto (**invited**)

Panelist, "Have We Entered a Brave New World of Global Content Takedown Orders?", Panel

organized by Harvard's Berkman Klein Center for Internet, RightsCon Summit, May 18, 2018, Toronto (**invited**)

Panelist, "Data Driven Decency: New, Collaborative Experiments to Diminish Online Hate and Harassment Online", Panel organized by Harvard's Berkman Klein Center for Internet and Society, RightsCon Summit, May 17, 2018, Toronto (**invited**)

Panelist, "The surveillance tool we love to carry: Cell phones searches and privacy in the evolving legal landscape", Panel organized by Canadian Civil Liberties Association, RightsCon Summit, May 16, 2018, Toronto (**invited**)

"Chilling Effects and the DMCA? An Empirical Case Study on Copyright Enforcement Online", Intellectual Property Law Discussion Group, Faculty of Law, University of Oxford, May 8 2018 (**invited**)

"Chilling Effects: How Laws and Surveillance Impact Us Online", CITP Luncheon Speaker Series, Center for Information Technology Policy, Princeton University, March 27, 2018 (**invited**)

"Mitigating the Impact of Automated Legal Processes on Internet Users", Civil Servant Research Summit, Center for Civic Media, MIT Media Lab, Cambridge, MA, January 28, 2018 (**invited**)

Presenter/Panelist, "Cybersecurity and Human Rights in the Online World", Political Science in the Digital Age: International Political Science Association (IPSA/AISP) International Conference, Hannover, Germany, December 4-6, 2017 (**invited**)

"Chilling Effects: How Laws and Surveillance Impact Us Online", OII Brown Bag Lunch Speaker Series, Oxford Internet Institute, University of Oxford, September 7, 2017 (**invited**)

"The Comparative Dimensions of Regulatory Chilling Effects Online", Rump Session Talk, 6th Annual Workshop on Free and Open Communications on the Internet (FOCI), USENIX Security Symposium, Advanced Computing Systems Association (ACSA), Vancouver, B.C., August 14, 2017

"Documenting the Impact of Surveillance on Civil Society" (with Tabasum Akseer), Connaught Summer Institute on Monitoring Internet Openness and Rights, Munk School of Global Affairs, University of Toronto, July 12, 2017 (**peer reviewed**)

"Trade Secrets for Open Societies: Some Modest Proposals For Reform", Sixth Annual Intellectual Property Scholars Workshop, University of Ottawa, Ottawa, May 10, 2017 (**peer reviewed**)

"The Comparative Dimensions of Chilling Effects Online", Internet Law Work-in-Progress Conference, Santa Clara High Tech Law Institute, Santa Clara Law School, Santa Clara, March 4, 2017

Presenter/Panel Discussant, "Cyberwarfare and International Humanitarian Law", 12th Annual International Humanitarian Law Conference, Schulich School of Law, Dalhousie University, January 27, 2017 (**invited**)

"Chilling Effects: Online Surveillance and Wikipedia Use", Privacy Law Workshop, Faculty of Law, University of Toronto, Toronto, November 19-20, 2016

Speaker Series Lecture, "Mass Hacking and the New Transparency: Legal and Public Policy Implications", Information Technology Policy Speaker Series, Computational Social Science Institute / Faculty of Computer Science, University of Massachusetts (Amherst), November 4, 2016 (**invited**)

"New Transparency Challenges", Connaught Summer Institute on Monitoring Internet Openness and Rights, Munk School of Global Affairs, University of Toronto, July 7, 2016 (**peer reviewed**)

Moderator / Discussant, "Privacy, the Internet, and the Right to be Forgotten", European Union Center for Excellence (EUCE) / Canadian International Council (CIC), Dalhousie U., April 20, 2016

"Chilling Effects: Insights on how laws and surveillance impact people online", Berkman Luncheon Series, Berkman Klein Center for Internet & Society, Harvard University, April 27, 2016 (**invited**)

"Chilling Effects and the DMCA? An Empirical Case Study on Copyright Enforcement Online", Internet Law Work-in-Progress Conference, New York Law School, New York City, March 5, 2016

Panel Discussant, "The Trans-Pacific Partnership: Economic, Social and Legal Implications for Atlantic Canada", Canadian International Council (CIC)/ Centre for Foreign Policy Studies, Dalhousie University, Delta Barrington, Halifax, March 2016

"Chilling Effects: Online Surveillance and Wikipedia Use", Cornell Law Society for Empirical Legal Studies (SELS) Global Junior Empirical Legal Scholars Workshop, Hebrew University, Jerusalem, Israel, December 2015 (**peer reviewed**)

Panel Discussant, "CETA: Intellectual Property Law Implications", CETA on the Brink? Post-Politics and the Finalization of the Canada-EU Trade Deal, European Union Center for Excellence (EUCE) / Canadian International Council (CIC), Dalhousie University, November 13, 2015

"Online Surveillance and Chilling Effects, 5th Annual Workshop on Free and Open Communications on the Internet", 2th Annual Free and Open Internet Communications (FOCI) Workshop, USENIX Security Symposium, Advanced Computing Systems Association (ACSA), Washington, D.C., August 10, 2015 (**invited**)

"Network Interference and Censorship Measurement: Ethical and Legal Issues", Connaught Summer Institute on Monitoring Internet Openness and Rights, Citizen Lab, Munk School of Global Affairs, University of Toronto, June, 27, 2015 (**peer reviewed**)

"Chilling Effects? Wikipedia Use and Online Surveillance", Fellows/Research Affiliates Discussion Group, Berkman Center for Internet & Society, Harvard University, May 6, 2015

"So... I Have This Genius Idea: Copyright, Trademarks, and Patents for Business and Innovative Ideas", (with Heather R Oke), Mixed Media Monthly: A Speaker Series About Art and the Business of Art, Artists Legal Information Society (ALIS), Art Gallery of Nova Scotia, April 16, 2015

"A Taxonomy of Chilling Effects", Internet Law Work-in-Progress Conference, Santa Clara High Tech Law Institute, Santa Clara Law School, Santa Clara, March 7, 2015

"Intellectual Property & NPOs: Issues, Suggestions, Best Practices", (with Alayna Kolodziechuk),

presentation to the Intellectual Property Law Section, Canadian Bar Association (Nova Scotia Branch), Pattersons LLP, January 16, 2015

"Internet Intermediaries and Corporate Transparency: The U.S. Experience", Connaught Summer Institute on Monitoring Internet Openness and Rights, Citizen Lab, Munk School of Global Affairs, University of Toronto, July, 29, 2014

"The Cycles of Global Telecommunications Censorship and Surveillance" University of Toronto—Osgoode Hall Law School Junior Scholars Workshop, Osgoode Hall Law School, April 25, 2014

Moderator / Discussant, "Transparency Reporting ", Transparency Working Group, Cyber Dialogue 2014: After Snowden, Whither Internet Freedom?, Canada Centre for Global Security Studies, University of Toronto, March 31, 2014

Moving Beyond Transparency Reporting: Internet Regulation & DMCA Parallels", Transparency Workshop, Boalt School of Law, University of California (Berkeley), November 19, 2013

Guest Lecture, "Copyright Law in Canada" Class: Law Information and Society (Prof. Bertrum MacDonald), School of Information Management, Dalhousie University, November 25, 2013

Panel Discussant, International Relations and Digital Technology Project, IDRTP Collective, Munk School of Global Affairs, University of Toronto, September 13, 2013 (**invited**)

"Early Weather Legal Report: Issues on the Horizon", 3rd Annual Workshop on Free and Open Communications on the Internet (FOCI), USENIX Security Symposium, Advanced Computing Systems Association (ACSA), Washington, D.C., August 13, 2013

"Welcome to Oz: Beyond a Black and White Debate on Internet Regulation (and Control)" (with Ryan Budish), Connaught Summer Institute on Monitoring Internet Openness and Rights, Citizen Lab, Munk School of Global Affairs, University of Toronto, July 22, 2013 (**invited**)

Panel Discussant, Transparency Reporting and Empirical Research in Intermediary Liability Standards Workshop, Institute for Information Law (IViR), University of Amsterdam, Amsterdam, NL, June 29, 2013 (**invited**)

Panel Discussant, Intermediary Liability and Freedom of Expression Roundtable, Institute for Information Law (IViR), University of Amsterdam, Amsterdam, NL, June 28, 2013 (**invited**)

Panel Discussant, "Cyberspace Governance: Exploring constitutive principles and values, today and into the future" Panel, Cyber Dialogue 2013: Governance without Governance in Cyberspace?, Canada Centre for Global Security Studies, University of Toronto, March 17-18, 2013 (**invited**)

"The Cycle of Global Telecommunications Technologies", Internet Law Work-in-Progress Conference, Santa Clara High Tech Law Institute, Santa Clara Law School, Santa Clara, March 16, 2013

"Internet Censorship and the Ghosts of Infowars Past", Berkman Center Luncheon Series, Berkman Center for Internet & Society, Harvard University, February 26, 2013 (**invited**)

"Doxxing, Hacker Culture, and the First Amendment" (with Molly Sauter), Berkman Fellows Hour, Berkman Center for Internet & Society, Harvard University, December 18, 2012

"Code as Speech and Other Challenges", Junior Scholars Workshop, Schulich School of Law, Dalhousie University, November 7, 2012

"Lessons for the Law & Politics of Internet Censorship Resistance Today" 2012-2013 Information Management Public Lecture Series, Faculty of Management, Dalhousie University, November 6, 2012 (**Invited**)

Commentator/Respondent, "Business Method Patents Are Coming to Canada", 42nd Annual Workshop on Consumer and Commercial Law, Schulich School of Law, Dalhousie , Oct 12-13, 2012

"Communications Disruption and Censorship Under International Law", 2nd Annual Free and Open Internet Communications (FOCI) Workshop of the 21st USENIX Security Symposium, Advanced Computing Systems Association (ACSA), Bellevue, Washington, August 8, 2012 (**peer reviewed**)

"Copyright's Media Theory and the Internet: The Case of the Chilling Effects Doctrine", Fifth Annual Intellectual Property Scholars Workshop, University of Ottawa, Ottawa, May 2012 (**peer reviewed**)

"Privacy Models for SenseCam (and Similar Research)" (with Paul Kelly), SenseCam2012: Third Annual Symposium, Exeter College, University of Oxford, April 3-4, 2012

Panel Discussant, Privacy and Financial Inclusion Conference, Birbeck College, University of London, London, UK, September, 2011

Panel Discussant/Moderator, "Copyright and Remix Culture", Remix Cinema Conference, University of Oxford, Oxford, UK, March 2011

"Open Connectivity, Open Data: Two Dimensions of the Right to Seek, Receive, and Impart Information in New Zealand", 2010 Annual Public Lecture in Cyberlaw, Faculty of Law, Victoria University of Wellington, Wellington, New Zealand, July 1, 2010 (**invited**)

Panel Discussant (and Co-organizer), "Public ACTA: Conference on the Anti-Counterfeiting Trade Agreement", Wellington Town Hall, Wellington, New Zealand, April 2010

Panel Discussant and Panel Co-Chair, "Copyright Future: Authors, Owners, Orphans, Users, and Repeat Infringers", New Zealand Centre for International Economic Law, Victoria University, October 2009 (**Invited**)

Panel Discussant, "Governance and Virtual Worlds", State of Play IV: Law and the Past, Present, and Future of Virtual Worlds, New York Law School, New York City, June 2009 (**invited**)

"The Emancipation Proclamation as a Constitutional Document", Cornell Law School Inter-University Graduate Conference, Cornell Law School, April 14, 2009

"The Evolving Approach to Section 15(1): Diminished Rights or Bolder Communities?" (with Roselyn J. Levine, Q.C.), 8th Constitutional Cases Conference, Osgoode Hall Law, York U. Toronto, April 2005

CURRENT GRANT FUNDED RESEARCH PROJECTS

PRINCIPAL INVESTIGATOR / CO-INVESTIGATOR (FUNDED)

Mitigating the Impact of Automated Enforcement Online
Princeton University / Massachusetts Institute of Technology / Dalhousie University

Fund: Artificial Intelligence Ethics & Governance Fund, MIT Media Lab
Amount: $154,736 CAD (125,000 USD) over 2 years (Fall 2017-2019)
Role: Co-Principal Investigator
Co-Investigators: Ethan Zuckerman, Associate Professor and Director, Center for Civic Media, MIT Media Lab; J. Nathan Matias, Postdoctoral Fellow, Princeton University; Merry Mou, a MIT Computer Science graduate student

This research project explores the impact of online platforms deploying algorithms and automated processes to enforce legal rights and obligations, monitor/surveil users, or police content and other online services, including testing legal, regulatory, and technological measures to mitigate negative side effects and, in the long run, protect people's rights and freedoms. We also expect to provide invaluable insights into how businesses and corporate platforms can more effectively employ these automated processes, while balancing business aims with user rights and consumer interests. Our methods are empirical, interdisciplinary, often collaborative with online platforms themselves, and use big data sources—like online platform data—and data analytics along with innovative and experimental research designs to do so. Our first case study in a series of such studies in collaboration tracks the impact of automated processes and "bots" enforcing copyrights online at mass scale under the U.S. Digital Millennium Copyright Act (DMCA). This study involves 100,000 social media users and documents the impact of these bots on users and platforms while testing different measures to mitigate any negative side effects like chilling effects and self-censorship. Other studies will look at automated content moderation on platforms, as well as biases in surveillance algorithms.

Toward a Public Interest Approach to Publicly Accessible Platform Data (FUNDED)
University of Ottawa / Dalhousie University / Ryerson University

Fund: Insight Grant, Social Sciences and Humanities Research Council (SSHRC)
Amount: $189,916 over 4 years (Fall 2018-2022)
Role: Co-Principal Investigator / Applicant
Co-Investigators: Teresa Scassa, Canada Research Chair in Information Law at University of Ottawa; and Pamela Robinson, Associate Professor, School of Urban and Regional Planning, Ryerson University

This is a multi-year SSHRC Insight grant funded project investigates the legal, ethical, and policy dimensions of publicly accessible platform data. This will include, among things, examining the issues of ownership, user rights, control, and privacy in relation to this data, and challenges raised by related emerging technologies and data practices like big data analytics, automated and algorithmic data scraping and processing, and automated platform content moderation. The project will confront issues of tort law, contract law, property law, as well as new and evolving forms of e-contracts, consumer protection, and commercial transactions

Connected Canada: Digital Citizenship in Canada Today (FUNDED)
University of Ottawa / Dalhousie University / University of British Columbia / Public Policy Forum

Fund: Connection Grant, Social Sciences and Humanities Research Council (SSHRC)
Amount: $24,592CAD over 1 year (Spring 2017-2018)
Role: Co-Principal Investigator / Applicant
Co-Investigators: Elizabeth Dubois, Assistant Professor, University of Ottawa; Alfred Hermida, Professor, School of Journalism, University of British Columbia; Florian Martin-Bariteau, Assistant Law Professor/Director, Center for Law and Technology, University of Ottawa

This is a multi-university, multi-partner SSHRC Connection grant used to fund a national conference to lay the foundations for a research agenda on "digital citizenship in Canada", including a significant technology law component. The October 2017 conference brought together academics across disciplines, policy makers, government officials, think tanks, civil society groups, and the private sector to investigate the internet Canada, including its history, emerging technologies, and applications, to understand what digital citizenship in Canada looks like, who is excluded from this vision, and how Canadian law and policy might respond.

PRINCIPAL INVESTIGATOR / CO-INVESTIGATOR (SUBMITTED)

Regulatory Gaps and Best Practices For a Rapidly Shifting Environment
Advanced Data Science Alliance (ADA)
Fund: Tri-Council Network Centres of Excellent Grant
Amount: $25 million over 5 years
Role: Co-Principal Investigator
ADA Scientific Co-Leads: Kelly Lyons (University of Toronto), Eleni Stroulia (University of Alberta), and Stan Matwin (Dalhousie University)
Theme Co-Leads: Lisa Austin, Professor of Law, University of Toronto; David Lie, Professor of Computer Engineering
Co-Principal Investigators: David Lyon, Professor of Sociology and Queen's Research Chair in Surveillance Studies, Queen's University; Ian Kerr, Professor of Law and Canada Research Chair, University of Ottawa

This project will be part of a large scale Tri-Council Networks Centres of Excellence project led by the Advanced Data Science Alliance (ADA), a multi-sectoral and trans-disciplinary national research network that, in partnership with industry and the public sector, will identify and address barriers to data-related innovation and enhance competitiveness in key sectors of the Canadian economy. There are 8 sub-themes in network, with law and policy addressed within the "Ethical, Accountable Technologies" sub-theme. The work on this sub-theme is led by University of Toronto's Lisa Austin and David Lie and aims to develop multidisciplinary approaches to new regulatory and ethical challenges for advanced data science methods, with special focus on emerging technologies like AI and machine learning, through research and training based on notions of corporate social responsibility and data justice. All Co-Leaders and Principal Investigators for the theme project are committed to multidisciplinary work and have academic backgrounds spanning law, philosophy, sociology, economics, computer engineering, and computer science. As well, the British Columbia, Alberta, and Federal Privacy Commissioners Offices will act as receptor partners for the grant and will help assist, support, and develop relating research, networking, and training opportunities.

COLLABORATOR

Internet Monitor and Transparency Project
Berkman Klein Center for Internet and Society, Harvard University

Fund: MacArthur Foundation
Amount: $1,242,760CAD over 5 years ($400,000USD 2013-2015; $600,000USD 2015-2018)
Role: Collaborator
Principal Investigator: Urs Gasser, Professor, Harvard Law School and Executive Director, Berkman Klein Center for Internet and Society, Harvard University

The award supports an applied research agenda to inform and shape policy development for governments and technology companies related to privacy, transparency, innovation, and security. The three areas of engagement include: 1) reducing privacy and security risks raised by private sector and government data sharing; 2) improving transparency and accountability associated with data acquisition and use by private companies; and 3) addressing harmful speech online. Currently building collaborative partnerships with private sector internet companies to broaden and standardize transparency reporting, to allow research on released data (in progress), including the impact of corporate surveillance and data disclosure. This also includes contributing to a large multi-faceted report on the impact of harmful speech online.

The Digital Copyright Takedown Project
Boalt School of Law, University of California (Berkeley) / Columbia University

Fund: Alfred P. Sloane Foundation and the Berkeley Digital Library Copyright Project
Amount: $1,517,924CAD over 6 years ($836,849USD 2011-2013; $384,565USD 2014-Present)
Role: Collaborator
Principal Investigators: Jennifer Urban, Professor, Boalt School of Law, University of California (Berkeley); Karaganis, American Assembly, Columbia University

A research project led by Jennifer Urban (Faculty of Law, UC Berkeley) and Joe Karaganis (American Assembly, Columbia University) that brings together range of scholars and researchers from universities around the world to collaborate on large-scale research project exploring intellectual property, copyright, and other intermediary liability enforcement systems and measures employed globally.

RECENT PAST GRANT FUNDED RESEARCH PROJECTS

PRINCIPAL INVESTIGATOR

CETA's Privacy and IP Implications for Canada
European Union Center for Excellence, Dalhousie University

Fund: European Commission
Amount: $10,000CAD (2015)
Role: Co-Principle Investigator / Applicant
Co-Investigators/Co-Applicant: Ruben Zaiotti, Director, European University Center for Excellence, Dalhousie University

This project, funded by the European Union (EU) (grant for funds succeeded via grant application in coordination with the European Union Center for Excellence at Dalhousie), examines the privacy and intellectual property law implications of the Comprehensive Economic Trade Agreement (CETA) between Canada and the EU. This grant funded participation in a symposium (examining trademark law/geographical indications under CETA), organizing/holding a conference on Europe's Right to be Forgotten (RTBF) in Canada,

and a report on CETA's implications for Canadian intellectual property laws.

Chilling Effects in the Digital Age: Three Case Studies
Doctoral Thesis, Oxford Internet Institute / Balliol College, University of Oxford

Funds: Doctoral Fellowship, Social Sciences and Humanities Research Council; Canada; Balliol College Graduate Student Bursary Fund; Canadian Centennial Scholarship Fund
Amount: $80,000CAD over 4 years ($20,000CAD/year, 2010-2014) along with miscellaneous amounts from year to year from the Balliol College scholarship and bursary funds;
Role: Principal Investigator / Applicant

My doctoral dissertation at Oxford explored the phenomena of regulatory chilling effects online through three empirical legal case studies, one involving the impact of online surveillance, another on the impact of the digital copyright enforcement online, and another survey-based study comparing the impact of different forms of online state actions/regulation. Primarily funded a SSHRC Doctoral Fellowship (converted from a CGS to take abroad).

PROJECT COORDINATOR

Privacy Value Networks (PVNets) Project
Oxford Internet Institute, University of Oxford

Fund: Engineering and Physical Sciences Research Council (ESPRC), United Kingdom
Amount: $2,534,953CAD over 4 years (£1,553,090, 2008-2012).
Role: Project Coordinator
Principal Investigator: Ian Brown, Professor, Oxford Internet Institute, University of Oxford
Collaborators: MA Sasse, Professor, University College of London; TNH Henderson, Professor, University of St. Andrew

A public and private sector research collaboration, funded by the UK's Engineering & Physical Sciences Research Council (EPSRC), on data privacy involving multiple universities and consulting firms. Coordinated all aspects of the project, including facilitating collaboration and communication among participants, organizing and chairing project meetings, formulating and administering project plan, monitoring deadlines, drafting and formulating project status reports, funding agency communications and relations, financial reporting, contracts, project deliverables, and their dissemination.

RESEARCH ADVISORY WORK

Ethics Feedback Panel for Networking and Security Research
Research Ethics Project, Microsoft Research, Cambridge, MA

Role: Panel Member / Collaborator
Principal Investigators: Stuart Schechter, Microsoft Research, Cambridge, MA and Bendert Zevenbergen, Postdoctoral Fellow, Princeton's Center for Information Technology Policy

The Networking and Security Research Ethics Feedback Panel (EFP) is an initiative led by Microsoft Research's Stuart Schechter. The EFP is a forum populated by volunteer experts in privacy, surveillance, and network security research that aims to help researchers identify ethics-related risks from their experiments and reduce these risks. The EFP encourages researchers to submit their research proposals for feedback prior to submitting them for

institutional review, so that they may integrate risk-reduction measures suggested by panelists and use panelists' feedback to inform institutional reviewers.

SELECTED MEDIA SPOTS / PRESS COVERAGE

I have been interviewed and quoted in media as an expert and my research received press coverage nationally and internationally, including the *Washington Post*, *New York Times*, *Newsweek*, *Reuters*, *TIME Magazine*, *NBC News*, *Le Monde*, *The Guardian*, *Forbes*, *Huffington Post*, *Politico*, *Slate*, *Motherboard*, *The Hill*, *The Globe and Mail*, *Toronto Star*, *CBC News*, *Global News*, *The Daily Mail*, *The Index on Censorship*, *Der Freitag*, *Il Fatto Quotidiano*, *The Times of India*, *Indian Express*, *Jerusalem Post*, as well as coverage by Pulitzer Prize winning journalist Glenn Greenwald in *The Intercept*.

Research covered in Lily Newman "The ACLU's Biggest Roadblock to Fighting Mass Surveillance" **WIRED Magazine**, June 29, 2018

Research covered in A.J. Marsden and William Nesbitt, "I Spy with My Little Eye: The Origins and Effects of Mass Surveillance" **Psychology Today**, November 6, 2017

Research covered / quoted in Tilman Bayer, "The chilling effect of surveillance on Wikipedia readers, and other recent research" in **Wikipedia Research Newsletter**, Vol 7:4, July 24 2017

Research covered / quoted in Peggy Sastre, "Sur Internet, les femmes et les jeunes s'autocensurent le plus", **Slate France**, July 16, 2017

Research covered in Tonya Riley, "Future Tense Newsletter: Trump's Idea for a U.S.-Russia Cybersecurity Unit Is Unbearably Dumb", **Slate Magazine**, July 12, 2017

Research covered in Gary Natriello, "The Chilling Effects of Surveillance", Ed Lab, Teachers College, **Columbia University**, July 12, 2017

Research covered in News, "Women and young people are hurt the most by internet surveillance — and it's getting worse", **Business Insider**, July 8, 2017

Research cited in John Naughton, "Google, not GCHQ, is the truly chilling spy network", **The Guardian**, June 18, 2017

Research recommended in Global Voices Advocacy, "In 'State of Emergency,' Internet Shutdowns Leave Ethiopians, Venezuelans Struggling to Connect", **Netizen Report**, June 1, 2017

Research covered / quoted in Jonathan Shaw, "The Watchers: Assaults on Privacy in America", **Harvard Magazine**, January-February, 2017

Research mentioned in Cynthia Wong, "The Dangers of Surveillance in the Age of Populism", **Newsweek**, February 2, 2017

Research covered in George Bowden, "Nine Important Stories of the Year That Slipped Under the Radar", **Huffington Post** (United Kingdom), December 27, 2016

Research mentioned in Henry Peck, "Speech Restrictions Cannot Be Wordplay", **Human Rights**

Watch (Dispatches Blog), October 26, 2016

Quoted in James Bradshaw, "Turkey's Erdogan uses FaceTime, social media to thwart military coup", **Globe and Mail**, July 26, 2016

Research covered in The Mackenzie Institute, "The Chilling Effect – How Mass Surveillance is Changing Your Online Behavior" (Video), June 26, 2016

Radio Interview (with host Dan Jones), "The Chilling Effect", **Radio Berkman 237**, Berkman Klein Center for Internet & Society, Harvard University, May 18, 2016

Research noted in Janus Kopfstein, "Lack of Online Privacy Has Chilling Effect, U.S. Department of Commerce Says", **Motherboard VICE**, May 14, 2016

Research covered in Brady Dale, "Humans Are the Best Sensors—Pairing Flickr With the News", **New York Observer**, May 6, 2016

Research covered / quoted in Annika Kremer, "Studie beweist Selbstzensur durch Überwachung", **Der Freitag** (Germany), May 6, 2016

Research covered / quoted in Tim Cushing, "The Chilling Effect Of Mass Surveillance Quantified", **Techdirt**, May 2, 2016

Research covered in News, "Traffic to Wikipedia Terrorism Entries Plunged After Snowden Revelations", **The Daily Mail** (United Kingdom), May 1, 2016

Research covered in News, "Study: Traffic to Wikipedia Terrorism Entries Plunged After Snowden Revelations", **Jerusalem Post**, May 1, 2016

Research covered in News, "Traffic to Wikipedia Terrorism Entries Plunged", **The Nation (Pakistan)**, May 1, 2016

Research covered / quoted in, News, "People Too Afraid To Search Privacy-Sensitive Topics After Snowden Revelations— Oxford Study", **Russia Today**, May 1, 2016

Research covered / quoted in Joshua Kopstein, "Snowden's Leaks Made People Less Likely to Read About Surveillance", **Motherboard**, April 30, 2016

Research covered in Yael Grauer, "Traffic to Wikipedia Entries Related To Terrorism Plummeted In Light of NSA Spying", **Forbes**, April 29, 2016

Research covered in Le Monde Pixels, "Traffic Après les révélations Snowden, moins de visites sur les pages Wikipédia sensibles", **Le Monde (France)**, April 29, 2016

Research covered in Amaelle Guiton, "Web : de la surveillance de masse à l'autocensure", **Libération (France)**, April 29, 2016

Research covered / quoted in Nieuws, "Als de staat meeluistert zijn burgers minder vrij", **Joop VARA** (Netherlands), April 29, 2016

Research covered / quoted in Glenn Greenwald, "New Study Shows Mass Surveillance Breeds Meekness, Fear, and Self-Censorship", **The Intercept**, April 28, 2016

Research covered / quoted in Marius Jorgenrud , "Færre leser om terror på Wikipedia etter Snowden-avsløringene, **Digi No** (Norway), April 28, 2016

Research covered in "Traffic to Wiki Terrorism Entries Plunged After Snowden Leaks", **Hindustan Times** (India), April 28, 2016

Research covered in News, "Traffic to Wikipedia terrorism entries plunged after Snowden revelations, study finds", **Reuters Africa**, April 28, 2016

Research covered in News, "Denúncias de Snowden fizeram cair tráfego de páginas sobre terrorismo na Wikipedia, entenda", **Tudo Celular** (Brazil), April 28, 2016

Research covered in Giulio Cupini and Fabio Scalet, "Privacy, lo spionaggio ci rende più ignoranti", **Il Fatto Quotidiano** (Italy), April 28, 2016

Research covered in News, "Internet Users Avoid Searching for 'Terrorism' on Web After Snowden Leak", **Sputnik News** (Russia), April 28, 2016

Research covered in Tim Starks, "Morning Cyber-Security Report", **Politico**, April 28, 2016

Research covered / quoted in Jeff Guo, "New Study: Snowden's disclosers about NSA spying had a scary effect on free speech", **Washington Post**, April 27, 2016

Research covered / quoted in Joseph Menn, "Traffic to Wikipedia terrorism entries plunged after Snowden revelations, study finds", Reuters (International), April 27, 2016

Research covered in NBC News Report, "Traffic to Wikipedia Terrorism Entries Plunged After Snowden Revelations", **NBC News**, April 27, 2016

Research covered / quoted in "Wikipedia Terrorism Entries Traffic Fell After Snowden NSA Reveal", **Newsweek Magazine**, April 27, 2016

Research covered in News, "Traffic to Wikipedia Terrorism Entries Plunged After Snowden Revelations, Study Finds", **The New York Times**, April 27, 2016

Research covered / quoted in Cory Bennett, "Snowden revelations had chilling effect on web browsing", **The Hill**, April 27, 2016

Research covered / quoted in Rudy Takala, "Study: Snowden leaks have made web users paranoid about what they browse", **Washington Examiner**, April 27, 2016

Research covered / quoted in Andrew Blake, "NSA surveillance has had a chilling effect on Internet browsing: report", **Washington Times**, April 27, 2016

Research covered in "Wikipedia traffic to terrorism entries plunge after Snowden revelations, study finds", **Business Insider**, April 27, 2016

Research covered / quoted in J. Nate Matias, "The Effects of Surveillance and Copyright Law on Speech: Jon Penney at Berkman", **MIT Center for Civic Media** (Blog), Massachusetts Institute of Technology, April 27, 2016

Research covered in News, "Consultas sobre terrorismo en Wikipedia bajan tras el escándalo de

Snowden: estudio", **Radio Fórmula** (Mexico), April 27, 2016

Research covered / quoted in Torsten Kleinz, "Studie zu Chilling Effects: Wikipedia-Artikel zu Terrorismus werden weniger gelesen", **Heise Online** (Germany), April 27, 2016

Research covered in News, "Wikipedia Pages on Terror See Traffic Plunge Post Snowden Leaks", **The Times of India**, April 27, 2016

Research covered in News, "Traffic to Wikipedia Terrorism Entries Plunged After Snowden Revelations: Reports", **Indian Express**, April 27, 2016

Research covered in News, "Security Revelations See Fall in Web Traffic – Study", **Otago Daily** (New Zealand), April 27, 2016

Research covered in News, "Wikipedia traffic to terrorism entries plunge after Snowden revelations, study finds", **ABC News** (Australia), April 27, 2016

Research covered in News, "Traffic to Wikipedia Terrorism Entries Plunged After Snowden Revelations, Study Finds", **Eyewitness News** (South Africa), April 27, 2016

Research covered in Esti Utami, "Setelah Pengakuan Snowden Pengakses Info Terorisme Menurun", **Suara News** (Indonesia), April 27, 2016

Research covered in News, "Wikipedia traffic to terrorism entries plunge after Snowden revelations, study finds", **Gulf Daily News** Online (Bahrain), April 27, 2016

Research covered in News, "Wikipedia traffic to terrorism entries plunge after Snowden revelations, study finds", **The Peninsula (Qatar)**, April 27, 2016

Research covered in "Traficul către paginile de Wikipedia dedicate terorismului a scăzut semnificativ după dezvăluirile lui Snowden (studiu)", **Agerpres** (Romania), April 27, 2016

Research covered in News, "Traffic to Wikipedia Terrorism Entries Plunged After Snowden Revelations, Study Finds", **The Express Tribune** (Pakistan), April 27, 2016

Research covered in News, "Traffic to Wikipedia terrorism entries plunged after Snowden revelations", **Free Malaysia Today**, April 27, 2016

Research covered in News, "Traffic to Wikipedia Terrorism Entries Plunged After Snowden Revelations, Study Finds", **Standard Media** (Kenya), April 27, 2016

Quoted in Robin Levinson King, "FCC met with Canadian researcher to understand CRTC", The **Toronto Star**, February 26, 2015

Quoted in Rebecca Lau, "Internet users receive illegal downloading notices, but what do they mean?", **Global News**, February 24, 2015

Quoted in Robin Levinson King, "Canadian viewers will get to see U.S. ads during 2017 Super Bowl", **The Toronto Star**, January 29, 2015

Quoted in M Donovan, "Failure to Connect: Nova Scotia's Digital Divide", **The Coast**, Oct 1, 2015

Quoted in: Sam Frizell, "Here's What Facebook Can Do With Your Personal Data in the Name of Science" **TIME Magazine** (July 7, 2014)

Quoted in "Elections Bill Exacerbates Lack of Privacy, Political Parties Micro Target Voters", The **Hill Times**, April 7 2014

Television Interview / Quoted in "NS Government hires Ontario lawyers to fight Bluenose II lawsuit:", **Global News (**TV), September, 2013

Quoted extensively in: Anonymous, "The Great Firewall of China", **Index on Censorship Uncut** Blog (15 March 2013)

ACADEMIC HONOURS AND DISTINCTIONS

2016 –
- Best Moot Team (Dalhousie), Best Oral Advocate (Gabby Lemoine, Dalhousie), Harold G. Fox IP Moot Competition, Toronto (Moot Team Coach / Supervisor)
- Research Affiliation, Civil Servant Project, MIT Media Lab (2018 – Present)
- Research Affiliation, CITP, Princeton University (2017 – Present)
- Research Fellowship, Citizen Lab, University of Toronto (20,000CAD) (2017 – 2018)

2013 – 2015
- Nomination, Law Students Association Award for Excellence in Teaching Law, Schulich School of Law, Dalhousie University (Spring 2015)
- Centennial Scholarship, Centennial Scholarship Fund, London, U.K. (2014)
- Research Affiliation, Berkman Klein Center for Internet and Society, Harvard University (2013 – 2015)

2012 – 2013
- Berkman Fellowship, Berkman Klein Center for Internet and Society (now Berkman Klein Center), Harvard University (2012 – 2013)
- Research Fellowship, Citizen Lab, University of Toronto (2012 – 2017)
- Research Affiliate, The Takedown Project, UC Berkeley Law; Eisenhower Institute, Columbia University (2013 – Present)

2010 – 2012
- Google Policy Fellowship, Citizen Lab, University of Toronto (7,500USD) (2011)
- 2011 Peter Oliver Prize in Canadian Legal History (c/o Osgoode Society/Law Society of Upper Canada) for "best article on Canadian legal history"
- Invited to give 2010 Annual Public Lecture on Cyberlaw at Victoria University of Wellington Law School, Victoria University, Wellington, New Zealand
- Social Sciences & Humanities Research Council Canadian Graduate Scholarship (converted to a Doctoral Fellowship to use abroad) (2010 – 2014)

2006 – 2009
- Harlan Fiske Stone Scholar Distinction, Columbia Law School (2009)
- Fulbright Scholarship, Canada-U.S. Fulbright Foundation (2008 –2009)
- Columbia Graduate Legal Studies Scholarship, Columbia Law School (2008 –2009)
- Lady Margaret Hall Award, University of Oxford (top student in the college's Social Sciences Division) (2007)
- Mackenzie King Travelling Scholarship, Mackenzie King Trust (2006 –2007)

2001 – 2003
- Tom Wilcox Award, Schulich School of Law, Dalhousie University (2003)
- Dean's List Distinction, Schulich School of Law, Dalhousie University (2003)
- Reviews Editor, Dalhousie Journal of Legal Studies, Dalhousie Law (2003)
- Dean's List Distinction, Dalhousie University (2000)

TEACHING

2012 – **Schulich School of Law, Dalhousie University**

Law and Technology (2014 – Present)
Upper Year Major Paper Seminar, Fall Term

Contract Law – Fall and Winter (2012— Present)
Mandatory First Year Course, Full Year)

Harold G. Fox Intellectual Property Moot (Coach/Supervisor) (2017 – Present)
Won top moot team and top mooter in first year participating (2017-2018)

Aboriginal and Indigenous Law in Context – (Facilitator) (2018 – Present)
First year 2 credit mandatory intensive course; I will facilitate, review, and engage student presentations as part of the Winter term module

Intellectual Property Law – (2012 – 2016)
Upper Year General Survey Course, Winter Term

2009 – 2010 **Faculty of Law, Victoria University of Wellington**

Internet Law and Regulation – Spring 2010
Upper Year / Graduate Seminar

GRADUATE SUPERVISION

Supervisor / Second Reader

Maria Dugas (Canada), LLM student, Thesis: "The Theoretical Case Against Criminalized Copyright Infringement in Canada" (Completed: 2017)

Ashwin Krishnan (India), LLM student, Thesis: "Towards an Effective Regime Against Online Copyright Infringement in India" (Completed: 2016)

Olefunke Salami (Nigeria), LLM student, Thesis: "Privacy Protection for Mobile Health (mHealth) in Nigeria" (Completed: 2015)

Farhan Raouf (Pakistan), LLM student, Thesis: "Modernizing Pakistan's Blasphemy Laws as Hate Speech" (Completed: 2014)

Directed Research Papers

Manal Alotiaba (Saudi Arabia), LLM student, "Anti -Cybercrime Law, Revenge Porn and Cyber Misogyny: A Comparative Analysis of the KSA, Canada, Egypt, and Pakistan" (Completed: 2018)

Liam Randhawa (Canada), "Luxury Fashion Brand Accessories: Perverting Trademark Law Theories" (Completed: 2016)

Examiner

Nick Hooper (Canada), LLM student, "Language's Empire: The Linguistic Foundations of Administrative Law" (Expected completion: Fall 2018)

PROFESSIONAL SERVICE

University Committees / Leadership

Director, Law and Technology Institute (September 2017 – Present)

Senator (Law School Rep.), Senate Standing Committee, Dalhousie U. (September 2017 – Present)

Chair, Information Technology Committee (2014 – Present)

Member: Research Committee (2012 – Present)

Member, Information Technology Committee (2012 – Present)

Associate, Jean Monnet European Union Centre for Excellence (2012 – Present)

Steering / Program Committees / Conference Chair

Steering Committee Member, Free and Open Communications on the Internet Workshop, USENIX Security Symposium, Advanced Computing Systems Association (2017– Present)

Co-Chair (with Nicholas Weaver of UC Berkeley), Free and Open Communications on the Internet Workshop (FOCI), USENIX Security Symposium, Advanced Computing Systems Association (ACSA) (2016-2017).

Program Committee: Free and Open Communications on the Internet Workshop, USENIX Security Symposium, Advanced Computing Systems Association (ACSA) (2012-2016)

Research Advisory Work

Member, Ethics Feedback Panel for Networking and Security Research, The Research Ethics Project, Microsoft Research, Cambridge, MA (2013 – Present)

PROFESSIONAL DESIGNATIONS AND MEMBERSHIPS

Bar Admissions

Law Society of Upper Canada, Province of Ontario, Canada (Year of Call: 2004)

New York State (Year of Call: 2013)

Professional Certifications

Certificate, Professional Training for Social Scientists, Saïd Business School, Oxford University

Certificate of Completion, Tri Council Policy Statement: Ethical Conduct for Research Involving Humans Course on Research Ethics (TCPS2: CORE)

Research Affiliations

Center for Information Technology Policy, Princeton University (2017 – Present)

Civil Servant Project, MIT Media Lab, Massachusetts Institute of Technology (2018 – Present)

Citizen Lab, Munk School of Global Affairs, University of Toronto (2012– Present)

Takedown Project, UC Berkeley Law / Columbia University (2012– Present)

Associate, Jean Monnet European Union Centre for Excellence (2012 – Present)

Organizations and Professional Membership

International Political Science Association (IPSA), Paris (since 2017).

Electronic Frontier Foundation (EFF), San Francisco, California (since 2012)

InternetNZ, Internet Society of New Zealand, (since 2009)

Oxford Union Debating Society (OUDS), University of Oxford (since 2007)

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 3

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, *Plaintiff*, v. NATIONAL SECURITY AGENCY / CENTRAL SECURITY SERVICE, *et al.*, *Defendants*.	No. 1:15-cv-00662-TSE

DECLARATION OF MICHELLE PAULSON

I, Michelle Paulson, declare:

1. I am a resident of San Francisco, California, over the age of eighteen. I have personal knowledge of the facts stated in this declaration and if called to testify I could and would testify competently thereto. I am providing this declaration in my capacity as a former employee of and current consultant to the Wikimedia Foundation, Inc. ("Wikimedia").

2. I am currently General Counsel at Redacted, and I serve as a consultant to Wikimedia. From July 2016 to May 2017, I was Interim General Counsel of Wikimedia, and from July 2015 to May 2017, I was a Legal Director for Wikimedia. I served as Senior Legal Counsel from November 2014 to July 2015, and as Legal Counsel from March 2010 to November 2014. I received my B.A. from the University of California, Berkeley and my J.D. from the University of California, Hastings. I am a member of the bars of the states of California and New York.

3. During my time with the Wikimedia legal team, I helped update and create Wikimedia's policies and guidelines related to user privacy and data retention. I also worked

closely with Wikimedia's engineers who were responsible for operationally implementing Wikimedia's data security protocols.

I. BACKGROUND

A. The Wikimedia Foundation

4. Wikimedia is a 501(c)(3) nonprofit charitable organization based in San Francisco, California, dedicated to encouraging the growth, development, and distribution of multilingual educational content, and to providing the full content of these "wiki"-based projects to the public free of charge.[1] Wikimedia operates twelve free-knowledge projects ("Projects") on the Internet, including Wikipedia, the world's largest and most popular encyclopedia.

5. Wikimedia provides the technical infrastructure for the Projects, which are primarily hosted on Wikimedia servers in Virginia, Texas, California, and Illinois. In addition, Wikimedia develops software and provides tools for others to build software platforms; develops mobile phone applications and has entered into partnerships with telecommunications companies; administers grants to support activity that benefits the Wikimedia user community and movement; provides administrative support to grantees; works with community members to organize conferences and community-outreach events globally; and engages in advocacy on issues that affect the Wikimedia community—which, at its broadest level, consists of individuals who access or contribute to the body of knowledge comprising the twelve Projects.

B. Wikipedia and Wikimedia's Other Free Knowledge Projects

6. The best-known of Wikimedia's Projects is Wikipedia—a free, multilingual Internet encyclopedia that is one of the most-visited websites in the world and one of the largest

[1] A "wiki" is a web application that allows collaborative modification, extension, or deletion of its content and structure.

collections of shared knowledge in human history. As of February 2018, the site has grown to contain more than 47 million articles in over 288 languages, and in 2017 it received more than 1 billion unique device visits each month. Wikipedia's content is collaboratively researched and written by millions of volunteers, many of whom choose not to identify themselves, and is in most instances open to editing by anyone with Internet access. Volunteers also use Wikipedia discussion forums and "Talk pages" to debate the editorial policies and decisions required for reliable and neutral content.

7. Other Projects include Wikimedia Commons, an online repository of free images, sound, and other media files; Wikibooks, a platform for the creation of free textbooks and annotated texts that anyone can edit consistent with the policies of the site; Wikinews, a collaborative journalism platform for volunteers to create and edit original news articles; and Wiktionary, a collaborative project for creating a free lexical database in nearly every language.

C. The Wikimedia Community

8. Wikimedia encourages individuals around the world to contribute to the Projects by communicating information to Wikimedia. Wikimedia receives and maintains this information, and subsequently communicates it to the many other individuals who seek to access, engage with, and further add to Wikimedia's archive of knowledge. The principal way in which Wikimedia communicates with its community is via the Internet.

9. Wikimedia maintains an active and close relationship with the volunteers, contributors, and many other users from around the world who comprise the Wikimedia community. Wikimedia users play a vital role in many of Wikimedia's functions and are active in the Foundation's initiatives, governance, and development of strategy. Wikimedia exists for its user community and depends upon it: users are responsible for the creation of content on the Projects, and users provide the readership base for the Projects. Both the creation of content and

engagement with that content are essential to Wikimedia's mission. In other words, Wikimedia operates interdependently with its user community in pursuit of a shared set of free-knowledge values.

10. This interdependence is reflected in Wikimedia's Board and decision-making structure. Roughly half of the members of Wikimedia's Board of Directors are selected by community members. The Wikimedia Board relies, in turn, on several user-staffed committees to oversee Board elections and recommend new Wikimedia chapters or community organizations. Community members serve on committees responsible for important organizational decisions, such as the Funds Dissemination Committee, which considers grant applications and provides substantive input on Wikimedia's annual plan, and the Language Committee, which proposes and coordinates Wikimedia projects in new languages. Moreover, the Wikimedia community is heavily involved in enforcing Wikimedia's community or project policies, which are largely created by the community. Privacy violations can be reported to an Ombudsman Committee, staffed by volunteers, and a volunteer-staffed Arbitration Committee handles escalated cases related to user conduct and abuse of policies. In sum, Wikimedia routinely makes core organizational decisions only after soliciting input and preferences of its users, including on topics such as its public-policy positions, the creation of new features and Projects, corporate strategy, and budgetary matters.

11. Community members around the world contribute to Wikimedia in other ways as well. The community provides Wikimedia with input on a variety of issues through a number of mailing lists hosted by Wikimedia. In addition, Wikimedia staff frequently engage in "Community Consultations," in which community members can offer their views on strategy, budget, public policy, and other matters directly. Wikimedia also receives significant financial

support from the community in the form of donations; affiliate organizations work with Wikimedia to help develop projects and allow Wikimedia fulfill its mission; and grantees (i.e., recipients of Wikimedia grants) perform important work to advance the Wikimedia movement. Community members are also deeply involved in the development and review of the computer code that supports the Projects.

12. Additionally, as stewards of the Wikimedia Projects and as reflected in Wikimedia's privacy policies, Wikimedia strives to protect the rights of users, including their right to express themselves, and to collaborate together globally, without fear of reprisal. As discussed in greater detail below, Wikimedia undertakes protective measures to ensure the security of its communications and the data it retains. It also resists third-party demands for users' information that are overly broad, unclear, or irrelevant; notifies users individually of information requests when legally permitted; and provides legal defense funds for certain community members who are subject to lawsuits or demands for non-public information as a result of their participation in the Wikimedia Projects.

II. WIKIMEDIA'S INTERNATIONAL INTERNET COMMUNICATIONS

13. "Upstream" surveillance conducted under Section 702 of the FISA Amendments Act ("Section 702") implicates at least three categories of Wikimedia communications: (i) Wikimedia communications with its community members, who read and contribute to Wikimedia's Projects and webpages, and who use the Projects and webpages to interact with each other; (ii) Wikimedia's internal "log" communications, which help it to monitor, study, and improve the use of the Projects; and (iii) communications of Wikimedia staff.

A. Communications of Wikimedia with Its Community Members

14. As the operator of one of the most-visited websites in the world, Wikimedia engages in an extraordinarily high volume of electronic communications with its users, who read

and contribute to Wikimedia's Projects and webpages, and who use the Projects and webpages to interact with each other. In 2017, Wikimedia sites received over 237 billion "page views," i.e., 237 billion instances of Wikimedia users visiting a particular page on Wikimedia websites, with approximately 74 billion views originating from users in the United States. Over the lifespan of the Wikimedia Projects, Wikimedia's users have edited its pages approximately 3.4 billion times. *See* Bayer Decl. ¶¶ 12, 21 (Exhibit 5). Each of these activities involves Internet communications between Wikimedia and its users—the majority of whom are located abroad.

15. Indeed, as explained in more detail in the Declaration of Tilman Bayer, Wikimedia engages in more than one trillion international communications each year, with individuals who are located in virtually every country on earth. For a user to view, search, log in, edit, or contribute to a Project webpage, the user's device must send at least one HTTP or HTTPS "request" to a Wikimedia server.[2] The number of requests required for a user to access a particular webpage depends on the number of graphics, videos, and other specialized components featured on the page. After receiving such a user request, the Wikimedia server transmits an HTTP or HTTPS "response" to the user's device, in which the content of the requested webpage component is rendered and displayed to the user. Between August 1, 2017 and January 31, 2018, Wikimedia's U.S. servers received approximately 381 billion HTTP or HTTPS requests from users outside of the United States. *See* Bayer Decl. ¶ 27. At this rate, Wikimedia engages in more than one trillion international HTTP or HTTPS communications each year.

[2] "HTTP" and "HTTPS" are common protocols for transmitting data via the Internet, including the content of many webpages. Unlike HTTP, which is unencrypted, "HTTPS" encrypts the connection between Wikimedia servers and the user's browser. *See* Bradner Decl. ¶¶ 120-23 (Exhibit 1).

16. Wikimedia also frequently engages in communications that permit its users to interact with one another more directly. For example, Wikimedia engages in communications that allow users to interact in small or limited groups—including over private and semi-private "wikis" that only certain users, such as user community leaders, can read or edit; private deliberations of user community leaders who help administer the Wikimedia websites; and Wikimedia mailing lists with restricted membership. Community members and leaders often debate and deliberate on organizational policies and decisions in the course of these communications. Separately, Wikimedia also enables registered users to send an email via Wikimedia to another registered user, so long as both have enabled email communications on their Wikimedia accounts. All of these interactions involve communications between Wikimedia and its community members.

17. Wikimedia's communications with its community members are often sensitive and private. Among other things, these Wikimedia communications link each user's page views, searches, and contributions to Wikimedia with his IP address, as well as with other user-specific information. As a rule, Wikimedia maintains as private the IP addresses associated with its community members and their individual interactions with the Projects. The sole exception is when an individual editor reveals his IP address publicly in conjunction with his edits. (Even when editors publicly disclose their IP addresses, many of their exchanges with Wikimedia—such as their page views, searches, and draft contributions—remain private.) *See* Bayer Decl. ¶¶ 12-16.

18. In other words, these communications contain some of the most sensitive information that Wikimedia possesses: which specific webpages each particular person is visiting or editing. They show who is reading—or writing—what. As a consequence, these

communications reveal a detailed picture of the everyday concerns of Wikimedia's users, and often constitute a record of their political, religious, sexual, medical, and expressive interests.

19. At times, these communications also contain questions, comments, or complaints that community members submit to Wikimedia about the performance and operation of its websites. And, at other times, they contain the private deliberations of user-community leaders who help administer the Wikimedia websites and, in that role, discuss Wikimedia's organizational policies and decisions.

20. Finally, Wikimedia's communications with its community members also reveal private information about its operations, including details about its technical infrastructure, its data flows, and its member community writ large.

21. Wikimedia's communications with its community members are essential to its organizational mission, as is its ability to control and maintain the privacy of these communications. Wikimedia's activities depend on its ability to ensure that readers and editors can explore and contribute to the Projects privately when they choose to do so. If these communications were not private, Wikimedia would have immense difficulty both gathering content and sharing information as widely as possible.

22. As a result, Wikimedia takes numerous, costly steps to protect the confidentiality of its communications, including through both legal action and technical measures, some of which are discussed in greater detail below. Wikimedia also assures its community via policies, public statements, and guidelines that it will reject third-party requests for non-public user information unless it is legally required to disclose that information. In keeping with these assurances, Wikimedia resists third-party demands for information that are overly broad, unclear, or irrelevant; notifies users individually of information requests when legally permitted; and

provides legal defense funds for certain community members who are subject to lawsuits or demands for non-public information as a result of their participation in the Projects. These steps are vitally necessary to fostering trust with community members and to encouraging the growth, development, and distribution of free educational content.

B. Wikimedia's Internal "Log" Communications

23. The second category of Wikimedia communications is its proprietary log communications, which it creates and transmits internally as part of its effort to monitor, study, and improve the Projects.

24. Every time Wikimedia receives an HTTP or HTTPS request from a person accessing a Project webpage, it creates a corresponding log entry. Among other private information, logs contain the user's IP address and the URL of the webpage sought by the user. Depending on the location of the user and the routing of her request, the log may be generated by Wikimedia's servers abroad, which in turn send the log to Wikimedia in the United States. Between August 1, 2017 and January 31, 2018, Wikimedia's foreign-based servers transmitted approximately 736 billion log communications to Wikimedia servers in the United States. *See* Bayer Decl. ¶ 27 (quantifying log communications). Wikimedia's proprietary log communications also reveal private information about its operations, including details about its technical infrastructure, its data flows, and its member community writ large.

25. Wikimedia's ability to control and maintain the privacy of its internal log communications is every bit as vital as its ability to ensure the privacy of its communications with community members. The interests described in paragraphs A.17 to A.22 above apply to these internal communications as well. Wikimedia's log communications provide a record of who Wikimedia associates with in the course of its activities, and reveal exactly what information Wikimedia is exchanging with the individuals who contribute to and visit the

Projects. Moreover, Wikimedia creates and transmits these log entries solely for its own internal purposes, as records of its activities, and it does not share them publicly. Because of the sensitivity of this information, Wikimedia seeks to collect and retain as little of it as possible. Indeed, Wikimedia takes steps to protect the confidentiality of these records and the sensitive information they contain—including by keeping them for only a limited amount of time, consistent with the maintenance, understanding, and improvement of the Wikimedia Projects and webpages and with Wikimedia's legal obligations. Still, Wikimedia possesses a large volume of sensitive information about its interactions with its community members, and it transmits a large volume of sensitive information about those interactions every day.

C. Communications of Wikimedia Staff

26. Wikimedia also engages in a third category of sensitive communications. Certain members of Wikimedia's staff routinely engage in sensitive, confidential, and privileged Internet communications with non-U.S. persons located abroad in carrying out Wikimedia's work.

27. Because Wikimedia's activities are global in scope, its staff's international communications are critical to its work. Many members of Wikimedia's U.S.-based staff routinely communicate with individuals abroad using a variety of different modes of electronic communication, including by email (Wikimedia email and Gmail), instant message (Google chat and Internet Relay Chat), video chat (Google Hangout and Skype), public and private "wikis," and an array of electronic third-party work-management tools that facilitate communications (Slack, Google Apps/G Suite, Trello, Sugar, Qualtrics, User Testing, and Salesforce).

28. Wikimedia's international contacts, many of whom are neither U.S. citizens nor permanent residents, include the following:

- Wikimedia's Board of Trustees, seven of whom are located abroad;

- Wikimedia's international contractors, over 140 of whom worked abroad in approximately 45 different countries, including India, Israel, Turkey, Russia, Poland, and Greece, between January 1, 2015 and December 22, 2017;

- Wikimedia's international outside legal counsel, which includes more than 30 law firms from over 20 countries, such as India, Russia, China, Egypt, and Chile;

- project partners and grantees, which encompass a broad spectrum of private-sector, non-profit, and governmental entities, including telecommunication companies, universities, education departments, libraries, and art galleries;

- foreign government contacts, including government officials and political and business leaders; and

- Wikimedia volunteers and other community members.

29. Many of Wikimedia staff's international communications are sensitive, confidential, and legally privileged. Because Wikimedia websites are viewed and edited by hundreds of millions of users all over the world, the organization is routinely confronted with a variety of complex legal issues in various countries. Thus, Wikimedia's U.S.-based attorneys frequently communicate electronically with international outside counsel—based in over 20 countries, including Finland, France, Germany, Greece, Hong Kong, India, Italy, Russia, and the United Kingdom—to discuss privileged matters. As a Wikimedia attorney, I regularly engaged in sensitive, confidential, and legally privileged communications with international outside counsel and Wikimedia contractors located abroad. A few examples of my work in these areas include the following:

- Beginning in 2014 and continuing through May 2017, I regularly communicated via email with Swedish counsel and foreign Wikimedia users in connection with a copyright infringement action involving the Swedish chapter of Wikimedia.

- In 2014 and 2015, I, along with other attorneys in the office, routinely corresponded with Wikimedia's counsel in Finland via email concerning Wikimedia's compliance with Finnish fundraising regulations.

- In 2012 and 2013, I communicated via email with counsel in China. In 2013, these discussions were focused on preparation for the annual Wikimedia conference, known as "Wikimania," which was held in Hong Kong.

- From 2013 through May 2017, I consulted with London counsel via email in connection with a variety of legal issues, including my work revising Wikimedia's internal privacy policies.

30. Wikimedia's U.S.-based legal team also communicates confidentially via the Internet with users abroad who have been threatened, harassed, detained, or sued in connection with their participation in Wikimedia activity, and with users who contact Wikimedia about privacy concerns and other personal matters involving the Wikimedia sites. For instance, I regularly retained and worked with foreign counsel in defending defamation actions involving Wikimedia and individual Wikimedia contributors. In 2014, I engaged counsel in Brazil to help defend against a defamation suit and subpoena seeking the identity of certain Wikimedia users who wished to remain anonymous. From 2012 to May 2017, I worked with Greek counsel to assist in the defense of a defamation action involving an individual Wikimedia user. In both cases, I regularly corresponded via email with users and their counsel.

31. Other members of Wikimedia's U.S.-based staff also engage in sensitive international communications, the confidentiality of which is essential to Wikimedia's work.

32. For example, Wikimedia's grant-making team communicates internationally on a regular basis concerning funding, organizational development, and support for users and volunteer groups who promote the Projects and Wikimedia's mission internationally. Some of these communications contain sensitive information such as personal bank account numbers, scans of photo identification, and private discussions of misconduct or other governance issues among grantees and potential grantees. The grant-making team's international communications also include discussions of volunteers whose work is considered controversial in their home countries—for example, in Venezuela, Iran, Ethiopia, Russia, Belarus, Saudi Arabia, and Kazakhstan. Because the exposure of this information could put volunteers and others in danger, the confidentiality of these communications is critical.

33. Likewise, when Wikimedia conference coordinators plan and promote an annual "Wikimania" conference, referenced above, Wikimedia staff communicate internationally about volunteers' and attendees' real names, email addresses, physical addresses, phone numbers, passport numbers, gender, age, and other affiliations. This information is particularly sensitive when it involves community members from countries of interest to the U.S. government.

III. UPSTREAM SURVEILLANCE OF WIKIMEDIA'S COMMUNICATIONS

34. The Declaration of Scott Bradner explains why it is a virtual certainty that the NSA is copying and reviewing Wikimedia's international communications—i.e., those with Wikimedia's community members, Wikimedia's internal log communications, and communications by Wikimedia staff—in the course of Upstream surveillance.

35. For the following reasons, I believe that it is very likely that Wikimedia is communicating with and about some of the thousands of people and organizations the government has targeted under Upstream surveillance—resulting in the retention of Wikimedia's communications.[3] Wikimedia's communications contain information that plainly falls within the scope of the U.S. government's foreign intelligence interests and its Section 702 collection, specifically.

36. First, Wikimedia routinely communicates with its users and other contacts in geographic areas that are a special focus of the U.S. government's counterterrorism or foreign policy efforts, such as Russia, India, and China. These international contacts have included

[3] At the time the Amended Complaint was filed in June 2015, the NSA used Upstream surveillance to collect communications to, from, and *about* its targets. The NSA reportedly suspended the collection of communications that are merely "about" its targets in April 2017 after violating court-imposed restrictions on Upstream surveillance. *See* Exhibit 45 (Press Release, NSA, *NSA Stops Certain Section 702 "Upstream" Activities*, Apr. 28, 2017, https://www.nsa.gov/news-features/press-room/Article/1618699/nsa-stops-certain-section-702-upstream-activities).

foreign telecommunication companies, such as Orange, Digicel, Airtel, and Beeline; foreign government officials; and hundreds of millions of Wikimedia users located abroad. Since 2011, Wikimedia staff have communicated with, among others, high-ranking leaders of Kuwait and Saudi Arabia; Wikimedia users in conflict zones such as Ukraine; and members of opposition movements throughout the world. Given the nature of Wikimedia's international contacts, and the fact that Wikimedia has hundreds of millions of international contacts, there is a substantial likelihood that at least some of these contacts are targets of Upstream surveillance.

37. Second, many of Wikimedia's international communications contain the kinds of "selectors"—communications accounts, addresses, and identifiers—that the NSA monitors. Hundreds of billions of Wikimedia's international communications (both its HTTP and HTTPS requests and responses, as well as its internal logs of user activity) include details such as website addresses and IP addresses. Furthermore, because Wikipedia is so comprehensive, it has encyclopedic entries for nearly any foreign company, government entity, or terrorist organization that the U.S. government would seek to target. Many of these webpages contain the kinds of selectors that the NSA monitors. For example, website addresses or domain names associated with organizations on the U.S. State Department's Foreign Terrorist Organization List are included on approximately 700 Wikimedia Project webpages—including webpages describing organizations, like Uzbekistan's Islamic Jihad Union, that have been the subject of investigations and prosecutions involving Section 702 surveillance.[4] Additionally, many staff communications contain email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to Wikimedia's work.

[4] *See United States v. Muhtorov*, 187 F. Supp. 3d 1240 (D. Colo. 2015).

38. Third, many of Wikimedia's international communications fall within the Section 702's broad definition of "foreign intelligence information." *See* 50 U.S.C. 1801(e). In addition to the numerous Wikimedia Project pages concerning foreign affairs, Wikimedia staff communicate about issues related to foreign affairs, as the following examples illustrate:

- Wikimedia launched a project called Wikipedia Zero, which was designed to offer Wikipedia free-of-charge on mobile phones in parts of the world where mobile is the primary (or only) means of access to the Internet, and mobile data costs pose a significant barrier to access. To form partnerships with telecommunications companies and to promote Wikipedia Zero, Wikimedia has communicated via email with foreign mobile-phone operators, foreign government officials, and others abroad. These communications include discussions of international law and the policies of foreign companies. Wikimedia has established Wikipedia Zero partnerships with telecommunications companies in more than 70 countries, including Bangladesh, Jordan, Kazakhstan, Pakistan, India, Russia, Saudi Arabia, Tajikistan, and Tunisia.

- Wikimedia is also routinely contacted by, and has been involved in legal action with, foreign government officials and political groups who have expressed dissatisfaction with certain content on Wikipedia pages. For example, in 2015 alone, Wikimedia staff communicated with, among others, government officials and high-ranking leaders of Turkey, Azerbaijan, and Saudi Arabia.

- Wikimedia employees regularly communicate with Wikimedia users from all around the world who are engaged in politically sensitive work or are involved in political opposition movements, including in locations such as Iran, Russia, Egypt, Ukraine, India, China, and Azerbaijan.

- Finally, members of Wikimedia staff also communicate internally about issues of national security and government compliance. For instance, Wikimedia's U.S.-based staff and foreign contractors correspond with one another, and with outside counsel, about the Office of Foreign Asset Control's Specially Designated Nationals List to ensure that Wikimedia's fundraising activities are in compliance with those restrictions.

IV. THE IMPACT OF UPSTREAM SURVEILLANCE ON WIKIMEDIA

39. Upstream surveillance has had a significant and long-lasting impact on Wikimedia's activities and operations.

40. Beginning in June 2013, there were numerous disclosures in the press and by the government concerning Upstream surveillance. The Washington Post and The Guardian were

the first to reveal Upstream surveillance to the public, and the government confirmed the existence of the program shortly thereafter. Over the course of the following year, the government provided additional information about this surveillance to the public.[5] Among the disclosures in the press, the Guardian and others published multiple NSA slides showing that the NSA was surveilling Wikimedia's communications to obtain intelligence information. One of these slides described analysts' ability to learn "nearly everything a typical user does on the Internet" by surveilling HTTP communications—and it identified Wikipedia as a prime example of the HTTP communications collected through NSA surveillance.[6] Another NSA slide published in July 2015 similarly showed that the NSA was intercepting Wikimedia's communications. In particular, it showed that the NSA had designed its search software to allow analysts to identify intercepted Wikimedia communications.[7]

41. These disclosures about Upstream surveillance and the NSA's surveillance of Wikimedia's communications, in particular, caused grave concern and alarm within the Wikimedia community and among Wikimedia staff.

---

[5] *See, e.g.*, Exhibit 15 (Privacy & Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of FISA* (July 2014)) (citing numerous official disclosures); Exhibit 17 (Office of the Director of National Intelligence, *DNI Declassifies Intelligence Community Documents Regarding Collection Under Section 702* (Aug. 21, 2013), http://icontherecord.tumblr.com/post/58944252298/dni-declassifies-intelligence-community-documents).

[6] *See* Exhibits 27 & 28 (Glenn Greenwald, *XKeyscore: NSA Tool Collects "Nearly Everything a User Does on the Internet"*, Guardian, July 31, 2013, https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data).

[7] *See* Exhibit 30 (*XKEYSCORE for Counter-CNE*, published in The Intercept on July 1, 2015, https://theintercept.com/document/2015/07/01/xks-counter-cne/ (Slide 9)) (describing computer code that identifies "wikimedia" and "wikipedia" HTTP communications); Exhibit 29 (Morgan Marquis-Boire, *et al.*, *XKEYSCORE: NSA's Google for the World's Private Communications*, Intercept, July 1, 2015, https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications) (publishing the *XKEYSCORE for Counter-CNE* slide deck).

42. As explained below, this surveillance has damaged Wikimedia's ability to carry out its mission by undermining the privacy and anonymity that both Wikimedia and its users depend on. In response, Wikimedia has undertaken a series of protective measures designed to mitigate the threat to its mission and better protect its communications against surveillance.

A. The Impact of Upstream Surveillance on Wikimedia's Users and Consequences for Wikimedia's Work

43. Confidentiality is essential to the work of Wikimedia staff and the organization as a whole. Wikimedia's work depends on the ability to ensure anonymity for individuals who view, edit, or use the Project pages and other Wikimedia websites. The ability to read, research, and write anonymously is essential to free expression and critical to Wikimedia's organizational mission.

44. The "ability of almost anyone to edit (most) articles without registration" is also considered a Founding Principle of Wikipedia. *See* Exhibit 31 (WIKI0008114). This Founding Principle has repeatedly been endorsed in Wikimedia's and the Wikimedia community's public statements. *See, e.g.*, Exhibit 32 (WIKI0006942) ("Privacy on the Internet is closely connected to our mission to disseminate free knowledge. We strive to provide a platform for users from all over the world to exercise their free expression right to share and study educational content. There are circumstances when contributors need to remain anonymous when working on the Wikimedia projects. To that end, the projects allow people to edit under a pseudonym, without providing any personal information, and without even creating an account. We want community members to feel comfortable when working on the projects. And we strongly oppose mass surveillance by any government or entity."); Exhibit 33 (WIKI0008108) ("The Wikimedia projects serve as a platform for people from all over the world to share and study knowledge. Sometimes, people may need to remain anonymous for personal or political reasons when

contributing to the Wikimedia projects. Wikimedia allows people to edit under a pseudonym, without providing any personal information, or without even creating an account. Anonymity and pseudonymity can protect people from retaliation for contributing to the Wikimedia projects."); Exhibit 34 (WIKI0008116) (community policies allow the creation of a second pseudonymous account for privacy purposes, given the importance of anonymity). The importance of anonymity to the Wikimedia community is also articulated in Wikimedia's official policy documents. For example, Wikimedia's Privacy Policy does not require users to create an account to read or contribute to a Wikimedia site, and users are not required to provide a "real name" to verify their identity during account creation. *See* Exhibit 35 (WIKI0006674).

45. Upstream surveillance undermines Wikimedia's ability to conduct its work. Notwithstanding Wikimedia's efforts to protect its information, NSA surveillance, including Upstream surveillance, has resulted and will result in some Wikimedia community members being less willing to engage with the Projects or with Wikimedia staff, because they fear that their communications will be intercepted by the U.S. government and also shared with other governments, intelligence services, and organizations with which the U.S. cooperates.[8]

[8] Users can face government scrutiny, coercion, and other forms of reprisal based on their association with Wikimedia. *See, e.g.*, Joe Sutherland, *2015 Wikipedians of the Year Unveiled in Mexico*, Wikimedia Blog (July 31, 2015), https://blog.wikimedia.org/2015/07/31/wikipedians-of-the-year-2015 (describing the Venezuelan government's revocation of the passport of a Wikimedia user for publishing photos of anti-government protests to Wikimedia). As another example, in March 2013, the Direction Centrale du Renseignement Intérieur ("DCRI"), a French intelligence agency, contacted Wikimedia and demanded removal of an entire Wikipedia article on the ground that it contained classified military information. After Wikimedia was unable to determine what information the DCRI considered classified or high-risk, the DCRI contacted a French Wikipedia volunteer with administrative rights. This volunteer had no role in the creation of the article; however, the DCRI insisted that he use his administrative rights to remove the article immediately, or face serious and immediate reprisals. In the face of these threats, the volunteer removed the article as authorities demanded.

46. For example, following disclosures about the nature and scope of NSA surveillance in the press in the summer of 2013, members of Wikimedia's community expressed fear and concern about Section 702 surveillance, prompting Wikimedia to hold an open "consultation" through an online forum. During this consultation, Wikimedia sought community feedback about the steps it should take to protect the privacy of Wikimedia's activities and its users from Section 702 surveillance. In response, Wikimedia's users from the U.S. and other countries discussed concerns about NSA surveillance activities, including Upstream surveillance. *See* Exhibit 13 (WIKI0008128, -8139) (one user commented on June 15, 2013: "[T]he NSA is also watching all strategic point[s] of internet across the world . . . . certain under sea cable landing have optical splittering [sic] circuits . . . ."). Users expressed their fears not only that their own activities were being surveilled, but also that the community as a whole would see a global drop in participation due to such fears. *See* Alexander Decl. ¶¶ 6, 11 (Exhibit 4).

47. The negative effects of Upstream surveillance on foreign users, described in more detail in the Declaration of James Alexander, are a direct detriment to Wikimedia, its ability to receive and distribute information, its organizational goal of increasing global access to knowledge, and its ability to associate privately with its community for all these purposes. Upstream surveillance also harms Wikimedia's domestic users, whose communications with Wikimedia's foreign servers are subject to this surveillance, and whose ability to exchange information and opinions with Wikimedia's foreign readers and contributors is impaired.

B. Wikimedia's Protective Measures in Response to Upstream Surveillance

48. Due in part to Wikimedia's and Wikimedia users' concerns about U.S. government surveillance, including Upstream surveillance, Wikimedia has undertaken a series of measures to protect its users, communications, and data, including adopting more secure methods of electronic communications, and in some instances self-censoring communications or

forgoing electronic communications altogether. These measures divert Wikimedia's time and monetary resources as a nonprofit entity from other important organizational work.

49. Due in substantial part to Upstream surveillance, Wikimedia transitioned from HTTP to HTTPS as the default protocol for all Wikimedia Project webpages. Historically, the Project websites used HTTP, not HTTPS, by default. However, revelations about Upstream surveillance in the summer of 2013 were a substantial factor in Wikimedia's decision to transition to HTTPS-by-default. As Wikimedia explained on its blog in August 2013, the release of the first NSA PowerPoint slide identifying Wikimedia as subject to U.S. surveillance "prompted our community members to push for the use of HTTPS by default for the Wikimedia projects."[9] On July 31, 2013, Wikipedia founder and Wikimedia Foundation Board of Trustees member Jimmy Wales cited this slide in a post on Twitter, stating that "NSA snooping on what YOU are reading at Wikipedia means I want us to go to SSL [the encryption protocol for HTTPS] sooner." Additionally, in his "State of the Wiki" address in Hong Kong in August 2013, Wales announced that Wikimedia would be transitioning to HTTPS-by-default due to revelations about NSA surveillance in June 2013. I was present for the "State of the Wiki" address and the video recording available at <https://www.youtube.com/watch?v=_w4oCslodDU> appears to be an accurate recording of the speech. Specifically, I recall Wales announcing that Wikimedia would be transitioning to HTTPS-by-default due to the revelations about NSA surveillance.

[9] *See* Exhibit 36 (WIKI0006700) (Ryan Lane, *The future of HTTPS on Wikimedia Projects*, Wikimedia Blog (Aug. 1, 2013), http://blog.wikimedia.org/2013/08/01/future-https-wikimedia-projects/); *see also* Exhibit 37 (WIKI0007108) (Yana Welinder, *et al.*, *Securing access to Wikimedia sites with HTTPS*, Wikimedia Blog (June 12, 2015), http://blog.wikimedia.org/2015/06/12/securing-wikimedia-sites-with-https/).

50. In order to effectively execute its transition to HTTPS-by-default for all Project pages, Wikimedia has devoted four years of full-time employee work allocated across different members of Wikimedia's staff. This transition to HTTPS-by-default has also created additional burdens on specific Wikimedia projects or initiatives. For example, the HTTPS transition necessitated approximately six months of full-time employee work to (1) coordinate with Wikimedia's partners regarding the manner in which the transition would affect the "Wikipedia Zero" project; and (2) provide related technical support.

51. Wikimedia initially had significant reservations regarding how the transition would affect users in large restricted corporate networks or users in countries such as China and Iran, for whom Wikimedia project webpages might or would become inaccessible if they were transitioned to HTTPS. Had it not been for revelations about the NSA's Upstream surveillance, it is likely that Wikimedia would not have transitioned all of its Project webpages to HTTPS-by-default, and instead would have relied on a less burdensome approach through which users could "opt-in" to using HTTPS. Revelations related to Upstream surveillance also contributed to Wikimedia's execution of the transition process on an accelerated basis. *See* Exhibit 38 (WIKI0002298) (statement on May 23, 2014 from Erik Möller, VP of Wikimedia Engineering and Produce Development: "Given increased concern about surveillance/monitoring, and our general commitment to protect user privacy, I expect we'll want to renew our emphasis on encryption and security, including: at least shifting search engine traffic to HTTPS via rel=canonical[;] . . . enabling IPSEC[;] investigating techniques to defeat traffic detection[;] making a definitive decision on whether to force HTTPS for all users.").

52. Due largely to Upstream surveillance, Wikimedia also implemented Internet Protocol Security ("IPsec"). IPsec is a secure network protocol suite that authenticates and

encrypts the packets of data sent over a network. To effectively execute IPsec implementation and maintenance, Wikimedia allocated approximately two years of full-time employee work.

53. Revelations about Upstream surveillance in the summer of 2013 prompted and was the decisive factor in Wikimedia's decision to implement IPsec. Wikimedia had considered implementing IPsec before the revelations, but only acted once it learned the extent of the NSA's surveillance practices as disclosed in June 2013. Knowledge that the NSA's Upstream surveillance involved tapping the Internet backbone made IPsec implementation necessary to protect the confidentiality and security of Wikimedia's communications. Revelations related to Upstream surveillance also contributed to Wikimedia's execution of the transition process on an expedited basis. *See* Exhibit 39 (WIKI0006564, -6566) (statement on July 8, 2013 from Tim Starling, Wikimedia Engineer: "For users geolocated in Europe, HTTPS connections are terminated in esams [Wikimedia's Netherlands server] and then the requests are forwarded unencrypted to eqiad [Wikimedia's U.S. server]. This compromises the security of the system. Recent news articles indicate that the physical security of the internet backbone may not be as good as previously assumed. I propose buying dedicated IPsec hardware for each DC, sufficient to encrypt cache-to-cache traffic and thus protect the privacy of our users.").

54. The transition to HTTPS-by-default and IPsec implementation required a capital expenditure on technical infrastructure:

(i) Wikimedia spent approximately €214,148.46 on Cache/TLS-termination servers located in Amsterdam, Netherlands.

(ii) Wikimedia spent approximately $40,384.56 on Cache/TLS-termination servers located in Virginia, U.S.A.

55. Wikimedia has also hired a full-time Traffic Security Engineer at a base salary of approximately €76,000, who will be responsible for implementing and maintaining technical efforts to protect Wikimedia users' reading and editing habits from mass surveillance—including, specifically, from the NSA's Upstream surveillance. *See* Exhibit 40 (WIKI0002344) (listing engineer's job responsibilities, the first of which is to "[p]rotect our users' reading and editing habits from mass surveillance").

56. Wikimedia's primary motivation in hiring a Traffic Security engineer is to maintain ongoing efforts to protect the confidentiality and security of its Internet communications in response to NSA surveillance practices, including Upstream surveillance. If it were not for Wikimedia's extensive efforts to combat the threat of NSA surveillance, Wikimedia would not have expended the additional resources to hire a new employee for this position.

57. In addition, as discussed in the Declaration of James Alexander, revelations about NSA surveillance, including Upstream surveillance, in the summer of 2013 led to a reluctance on the part of international community members to interact with U.S.-based Wikimedia staff. Fears over NSA surveillance of international Internet communications meant that Wikimedia was required to increasingly rely on in-person communications and encrypted messaging systems when interacting with community members. Due to NSA surveillance, including Upstream surveillance, Wikimedia staff have self-censored their speech and in some instances have forgone electronic communications altogether. *See* Alexander Decl. ¶¶ 13-14.

58. After the summer 2013 revelations about Upstream surveillance, Wikimedia also held internal discussions and community consultations specifically related to NSA surveillance. *See* Exhibit 13 (WIKI0008128) (Wikimedia community consultation on NSA surveillance

disclosures). Due in part to user concerns about Upstream surveillance, Wikimedia expedited the negotiation, drafting, and approval of a new Privacy Policy. *See* Exhibit 41 (WIKI0006602) (Wikimedia blogpost summarizing consultation process). Wikimedia staff responded to community concerns over surveillance—including concerns specifically about the NSA's Upstream surveillance—when drafting these policy changes. I assumed a lead role in developing these new privacy policies, which required extensive consultations and several months' worth of work.

59. Wikimedia is a non-profit organization with limited staff and financial resources. The aforementioned resources that Wikimedia devoted to protect the confidentiality of its communications were made at the expense of other organization initiatives and activities that Wikimedia could have undertaken to further advance its mission.

V. CONCLUSION

60. Freedom of speech, freedom of association, and access to information are core values for Wikimedia. As stewards of the Wikimedia Projects, Wikimedia strives to protect the rights of users, including their right to express themselves, and to collaborate together globally, without fear of reprisal. Many of the topics discussed on Wikimedia pages are controversial or politically sensitive. When Wikimedia's users are afraid to read about or contribute to the collective understanding of those topics, the organization's mission of providing free access to knowledge to all, including Americans, is threatened.

61. The intrinsic value of the Wikimedia Projects lies in both what they are and how they are built. They are an ever-expanding resource of information and ideas, created through open collaboration and dialogue. Upstream surveillance threatens that global collaboration and dialogue, and it does so without deference to the freedoms that ensure free and open access to knowledge for all.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on December 18, 2018 in San Francisco, California.

Michelle Paulson

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 4

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, *Plaintiff*, v. NATIONAL SECURITY AGENCY / CENTRAL SECURITY SERVICE, *et al.*, *Defendants*.	No. 1:15-cv-00662-TSE

DECLARATION OF JAMES ALEXANDER

I, James Alexander, declare:

1. I am a resident of Daly City, California, over the age of eighteen. I have personal knowledge of the facts stated in this declaration and if called to testify I could and would testify competently thereto. I am providing this declaration in my capacity as a former employee of the Wikimedia Foundation, Inc. ("Wikimedia").

2. I graduated from the University of Rochester in 2010 with a Bachelor of Arts in Economics. I have been a volunteer editor on Wikimedia projects since November 2006 and worked professionally at Wikimedia from August 2010 until December 14, 2018. As an employee at Wikimedia, I worked with Trust and Safety investigations and community management, and in June 2013, I became a full-time Manager for Wikimedia.

3. Beginning in August 2015 until December 14, 2018, I was the Manager for Trust and Safety at Wikimedia. Between June 2013 and August 2015, I was Manager of Wikimedia's Legal and Community Advocacy team. As Manager for Trust and Safety at Wikimedia, I focused on liaising and working with Wikimedia community members who have special administrative responsibilities requiring high levels of trust, including users who have access to private data and

other sensitive information. I also worked on threats of harm to community members or the public that arise in the context of the twelve free-knowledge projects ("Projects") that Wikimedia operates. As Legal and Community Advocacy Manager, I occupied a similar role, coordinating community consultations on new Wikimedia policies and procedures, and acting as primary investigator on threats to community members and other members of the public.

I. Impact of Upstream Surveillance on Wikimedia and its Community Members

4. Since the public first became aware of Upstream surveillance in June 2013, Wikimedia community members have been less willing to read, contribute to, or otherwise engage with Wikimedia Projects and Wikimedia staff online. Due to NSA surveillance, including Upstream surveillance, numerous Wikimedia users around the world have expressed their reluctance to participate in the Wikimedia movement, to read and edit Wikimedia pages, and to share information or communicate with Wikimedia's staff. Wikimedia users have done so in a variety of ways and settings, including but not limited to Wikimedia community forums, Wikimedia discussion groups, and in communications with Wikimedia employees. After the public revelations about Upstream surveillance began in June 2013, Wikimedia staff received numerous complaints about NSA surveillance from users in the United States and around the world. In dozens of these complaints, which occurred in person or through Internet messaging applications, community members either specifically referenced Upstream surveillance by name or the context made clear that they were referring to Upstream surveillance as the basis for their concern.

5. The impact of NSA surveillance—including Upstream surveillance—on Wikimedia community members has taken several forms.

6. Wikimedia staff, myself included, have had numerous conversations with Wikimedia users in the United States and abroad who have self-censored their speech with Wikimedia, or altered or limited their engagement with Wikimedia due to NSA surveillance, including Upstream

surveillance. Many of these individuals are involved in political or social activism and live or work in geopolitical areas that are a special focus of the U.S. government's counterterrorism or foreign policy efforts, such as Iran, Russia, Egypt, Ukraine, India, China, and Azerbaijan. These individuals have engaged in repeated acts of self-censorship vis-à-vis Wikimedia because of NSA surveillance: some refuse to discuss sensitive political topics on which they once spoke candidly; some will now only speak in person rather than over email or other communication channels they used to use; and some will only speak through intermediaries. Users fear NSA surveillance, including Upstream surveillance, and the consequences of that surveillance. In particular, they fear information about their activity on Wikimedia sites could, among other things, identify them, jeopardize or undermine the political or social movements in which they work, or otherwise result in harm to themselves or their families. Many of them were especially concerned about their online activity on Wikimedia project pages because of published NSA slides showing that the NSA was surveilling Wikimedia communications in order to obtain intelligence information. *See* Exhibit 8 (WIKI0006462, -6471-73) (Wikimedia-hosted email list discussing NSA slide with Wikimedia logo).

7. Due in part to concerns about U.S. government surveillance, including Upstream surveillance, some Wikimedia community members abroad have self-censored their speech by refusing to transmit photo identification to Wikimedia staff over the Internet. To gain access to certain tools and access privileges for Wikimedia Projects, community members were historically required to send Wikimedia a copy of their official government-issued identification so that their identities could be confirmed. On several occasions since the public first became aware of Upstream surveillance, users have told Wikimedia that they would not transmit photo identification to Wikimedia via the Internet because of concerns about U.S. government

surveillance. One user stated in a community consultation about Wikimedia's privacy-related policies, "I am . . . very concerned and feel deeply uneasy about (re-)sending a copy of my ID—which is probably one of the most delicate information the WMF can hold—to an organization in a country where countless government agencies can force them to reveal any and all information they want, or even get the information without a court's approval or the subject's awareness. (Yes, I'm looking at the U.S., the recent scandals around the NSA, and the worryingly broad scope of the CIA and other intelligence-gathering organisations.)" *See* Exhibit 9 (WIKI0006410, -6417). These refusals by users to transmit photo identification to Wikimedia due in part to concerns about NSA surveillance have directly affected Wikimedia's ability to carry out its work. They have forced Wikimedia staff to find other, less convenient ways to review community members' identification, including via in-person meetings with international community members.

8. Similarly, due to NSA surveillance, including Upstream surveillance, Wikimedia community members have expressed reluctance to share private data when seeking Wikimedia's assistance in making arrangements to attend Wikimedia conferences or events. Trust and Safety and other teams have also operated through intermediaries when communicating with users in countries of interest to U.S. intelligence agencies, in an effort to avoid surveillance of text-based Internet communications.

9. In addition, certain community-elected users with advanced access to Wikimedia tools and settings, known as "stewards," have avoided email communications with Wikimedia due to NSA surveillance, including Upstream surveillance. Historically, stewards communicated via email regarding a variety of issues arising from Wikimedia's activities, including sensitive conversations about perceived threats to the safety and security of community members. However, after the public first became aware of Upstream surveillance in the summer of 2013, the stewards

expressed reluctance to communicate via email regarding sensitive issues. Thus, in order to work with the stewards on sensitive topics, Wikimedia began to hold regular encrypted videoconference meetings with the stewards.

10. As another example, due to NSA surveillance, Wikimedia community members have sought to use special applications that completely anonymize their communications with Wikimedia. To maintain the integrity of content on Wikipedia, Wikimedia does not permit users with editing privileges to rely on software such as Tor—an Internet browser application that helps anonymize communications online—to shield their IP addresses from Wikimedia. Since the public first became aware of Upstream surveillance in June 2013, Wikimedia community members abroad, including American citizens, have increasingly requested exceptions to this policy as part of efforts to avoid NSA surveillance activities. *See* Exhibit 10 (WIKI0009221, -9222) ("I am a US citizen living abroad. According to recent news reports this places me in a category for elevated surveillance by my government . . . . I prefer to minimize such invasions of my privacy and so use TOR where possible. The global block on TOR exit points has reduced my spontaneous contributions to the WMF projects I am still somewhat involved with."); Exhibit 11 (WIKI0009218, -9219) ("I would like to use Tor while editing Wikimedia wikis, but it seems Wikimedia blocks all Tor exit nodes. . . . I am concerned that [the Philippines] will take hard measures like spying on Filipino citizens and collaborating with the NSA. That's why I am using Tor to prepare if this happens."). I have also had in-person conversations with users who have stated that they would not feel comfortable contributing to or editing Wikimedia pages without using anonymizing software.

11. Wikimedia users have also expressed their concerns about NSA surveillance—and how that surveillance deters users from participating in Wikimedia Projects—through Wikimedia

community forums and similar web pages. Wikimedia hosts a number of forums and other pages in which Wikimedia users converse on a range of topics, including their use of, and participation in, Wikimedia Projects. For example, in December 2013, a group of over 100 users from the German Wikipedia community specifically mentioned NSA surveillance when discussing proposed revisions to Wikimedia policies related to user data. *See* Exhibit 12 (WIKI0001474, -1476) ("The revelations by Edward Snowden and the migration of programs from the Toolserver to Tool Labs prompted discussions among the community on the subject of user data and how to deal with it."). As another example, on a user "Talk page" about the implications of NSA surveillance, one community member stated: "Wikimedia relies on editors being able to edit freely without real world retaliation. This is one reason thinks [*sic*] like no legal threats is a policy. If editors fear retalation [*sic*] by gov for the things they do on Wikimedia, they wont do things that might piss off gov . . . . Obviously we arent at a full surveillance/police state yet, but things like that happen one small step at a time. This is a large step." *See* Exhibit 13 (WIKI0008128, -8144). Indeed, users feared U.S. surveillance of their communications and the potential consequences. Because of NSA surveillance, including Upstream surveillance, many Wikimedia users indicated to me and other Wikimedia staff in conversations in person and through encrypted messaging applications that they feared not only participating in Wikimedia Projects as contributors or editors, but also even reading or visiting Wikimedia pages. They feared NSA surveillance of their communications with Wikimedia and the consequences of that surveillance. In particular, they feared that the information could be used by the U.S. government to reveal users' identities, to identify their political or social activism, or to detect anti-American bias.

12. When users self-censor their speech or otherwise limit their engagement with Wikimedia, it directly harms Wikimedia's ability to carry out its mission to develop and disseminate free

educational content. This disengagement also interferes with the work of Wikimedia staff, discussed in more detail below.

II. Interference with the Work of Wikimedia and its Staff

13. Due to NSA surveillance, including Upstream surveillance, Wikimedia staff have self-censored their speech and in some instances have forgone electronic communications altogether. NSA surveillance, including Upstream surveillance, has made it more difficult for Foundation staff to receive information from and effectively respond to community members—an essential part of running an international community-based organization like Wikimedia. Wikimedia staff have been forced to rely more heavily on in-person meetings and encrypted messaging systems to preserve the confidentiality and security of their communications. As a result, Wikimedia has suffered harm to its institutional goals.

14. Since the public became aware of Upstream surveillance in June 2013, Wikimedia staff on the Trust and Safety team have traveled to attend international Wikimedia conferences more frequently to communicate about sensitive issues in person with community members who are concerned about NSA surveillance, including Upstream surveillance, of their Internet communications. The Trust and Safety team sent at least two additional staff members to each of the annual "Wikimania" conferences held from 2014 through 2018; these conferences are held at locations around the world and the cost of attendance can reach several thousand dollars per staff member. Wikimedia has also sent additional staff each year to attend the "Wikimedia Conference" in Berlin to communicate about sensitive issues in person. Finally, members of the Trust and Safety team have more frequently attended additional country-specific conferences, especially in locations around the world where community members have expressed concerns about NSA surveillance, including Upstream surveillance, such as Germany, Austria, the Middle East, and Eastern Europe. I was personally involved in the decision to send more Wikimedia staff to attend

these events, and the decision was strongly influenced by the fact that Wikimedia community members and affiliate organizations were not comfortable having sensitive conversations online about issues crucial to Wikimedia's mission.

15. Forgoing email and other forms of text-based Internet communications has other adverse consequences on Wikimedia staff. The use of encrypted messaging systems often requires staff to publicly disclose their personal contact information when they otherwise would not have done so. For example, one encrypted messaging system that I frequently used to communicate with community members and other international staff—WhatsApp—requires that I disclose my mobile phone number for account verification. Because Wikimedia lacks the resources to provide staff with mobile phones and data plans, I disclosed my personal mobile phone number to community members in order to use WhatsApp, when I would otherwise not have done so.

16. Due to Upstream surveillance, the Trust and Safety team cannot communicate and operate as effectively worldwide.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on December 17, 2018 in San Francisco, California.

James Alexander

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 5

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, *Plaintiff*, vs. NATIONAL SECURITY AGENCY / CENTRAL SECURITY SERVICE, *et al*., *Defendants*.	No. 1:15-cv-00662-TSE

DECLARATION OF TILMAN BAYER

I, Tilman Bayer, declare:

1. I am a resident of San Francisco, California, over the age of eighteen. I have personal knowledge of the facts stated in this declaration and if called to testify I could and would testify competently thereto. I am providing this declaration in my capacity as an employee of the Wikimedia Foundation, Inc. ("Wikimedia").

2. I am a Senior Analyst in Wikimedia's Product Analytics team, and have been a full-time employee of the organization since 2012. My responsibilities include the reporting of pageview statistics and other key web traffic metrics to Wikimedia's executives and board. I hold degrees in mathematics from the University of Cambridge (Certificate of Advanced Study in Mathematics) and the University of Bonn (diploma, equivalent to a Master's degree in the US).

3. As explained in further detail in the Declaration of Michelle Paulson (Exhibit 3), Wikimedia is a 501(c)(3) nonprofit organization dedicated to encouraging the growth, development, and distribution of multilingual educational content, and to providing the full content

of these "wiki"-based projects to the public free of charge.[1] Wikimedia operates twelve free-knowledge "Projects" on the Internet, including Wikipedia, a free-access, free content encyclopedia that is the Internet's largest and most popular reference work, and one of the top ten most-visited websites in the world. At the time of the filing of the Amended Complaint in 2015, Wikipedia received more than 400 million visitors each month. *See* Exhibit 44 (WIKI0008271). As of February 2018, the site has grown to contain more than 47 million articles in over 288 languages, and in 2017 it received visits from more than 1 billion unique devices each month.

4. Wikimedia performs a variety of activities that support the Wikimedia movement. Most relevant to my testimony here, Wikimedia provides technical infrastructure for the Projects, and operates over 1000 servers located in the United States, in the Netherlands, and since March 2018, in Singapore. In response to Defendants' written discovery requests in this litigation, I was tasked with quantifying the volume of Internet communications that are transmitted by Wikimedia's servers. My analysis quantified communications by overarching category, Internet protocol, and country of origin. The results of these analyses were produced during discovery. *See* Exhibits 14, 42, and 43. I also quantified and verified other statistics relevant to the volume of Wikimedia's communications, a subset of which are produced herein. *See infra* ¶ 29.

I. TECHNICAL BACKGROUND

A. HTTP/S Requests and Responses

5. A brief description of how computers communicate over the Internet is helpful to understanding the nature of Wikimedia's communications with its users. More fulsome explanations of these technical processes are provided in the expert Declaration of Scott Bradner (Exhibit 1).

[1] A "wiki" is an application that allows collaborative modification, extension, or deletion of its content or structure.

6. The hypertext transfer protocol, or HTTP, is the foundation for data communication over the world wide web and facilitates the exchange of information between computers. HTTP is a "request/response" "Application Layer" protocol that governs how communications occur between "clients" and "servers." A "client" is often a software application, such as a web browser, that initiates a request to connect with a "server," which may be a computer hosting a website. To access a particular webpage, a client must send at least one HTTP request to the relevant server. The number of requests required for an Internet user to access a particular webpage depends on the number of graphics, videos, and other specialized components featured on the page. A server responds to a request by providing the requested "resource." Uniform Resource Locators, or URLs, both identify a resource and describe its location or address. When an Internet user enters a URL address into their web browser using the "http" or "https" web address format, or when a user clicks on a "link" to a webpage, they are actually instructing their web browser (the client) about which resource to request and where to find it.

B. HTTPS and Wikimedia Projects

7. Hyper Text Transfer Protocol Secure (HTTPS) is the secure version of HTTP. Web browsers use the URL convention of replacing "http:" with "https:" to indicate that the browser is to communicate with the web server using the "Transport Layer Security" (TLS) protocol instead of the unencrypted protocol used by HTTP. HTTPS operates between the application and transport layers, and encrypts the HTTP application layer communication.

8. Over the past several years, Wikimedia has transitioned to the use of HTTPS by default. *See* Paulson Decl. ¶¶ 49-50. Currently, HTTPS is enabled on all Wikimedia Project websites. If a user requests a Wikimedia site using "http:" in their web browser, they receive a "redirect" response from Wikimedia's servers, which includes the URL information from the user's request.

C. Other Internet Communications Protocols

9. The Transmission Control Protocol (TCP) is a transport layer protocol used to provide a reliable data stream between network nodes. It is used by most major Internet applications including email and the world wide web.

10. The User Datagram Protocol (UDP) is a transport layer protocol that provides a way to send packets from one network node to another network node. Many applications use UDP for transport including some voice and video streaming applications.

11. The Internet Control Message Protocol (ICMP) is a supporting communications protocol used by network devices, including routers, to send operational information, including error messages.

II. WIKIMEDIA PROJECT PAGES AND FEATURES

A. Editing Project Pages

12. All twelve of the Wikimedia Projects are written, edited, and curated collaboratively online by volunteers. Wikimedia users can contribute to Project websites anonymously, under a pseudonym, or under a username that reflects their real identity. As of March 2018, there have been approximately 3.4 billion edits over the lifespan of the Wikimedia Projects.

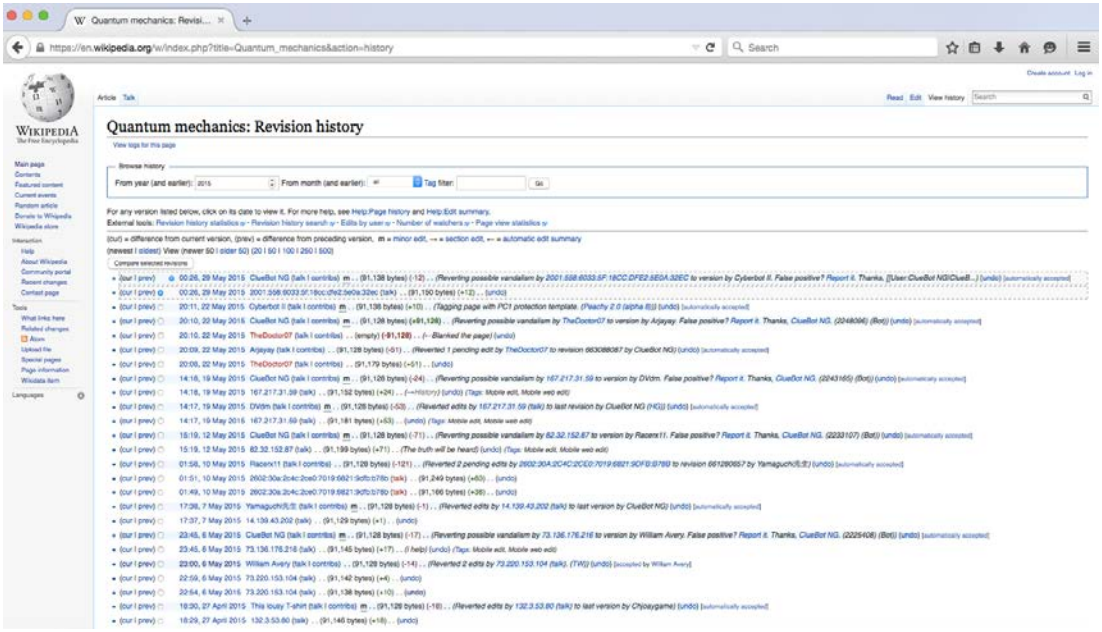
13. Users can edit a specific Wikimedia Project page via an "Edit" page, which contains a text box with an editable version of the article. An example of an Edit page is depicted in Figure 1 below.

Figure 1

14. Any revisions on this edit page will generally remain private until the user selects the "Publish changes" option (earlier named "Save page" or "submit changes") at the bottom of the screen. If a user selects "show preview" while editing a draft, the changes are communicated between the user's browser and Wikimedia's servers. After the user saves her changes, the user's revisions are publicly visible on the page.

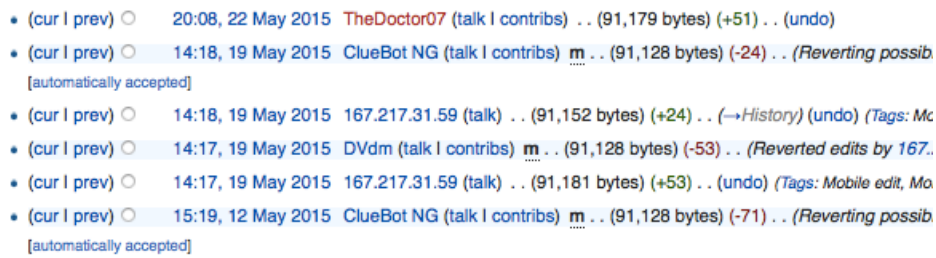
15. The revision history for every page on each of the twelve Projects is publicly visible by clicking on the "View history" or "History" tab on the right side of the screen. This revision history includes unique edits made by individual users. An example of a revision history page is depicted in Figure 2 below.

Figure 2



16. Figure 3 displays a portion of the revision history of the Wikipedia page on "Quantum mechanics." As illustrated in this Figure, when a user who is not logged in as a registered user edits the article, the user's IP address information is visible next to a link to the contributions from that IP address. When a user contributes while logged in to his account, the corresponding revision history page does not reveal the user's IP address. Instead, the revision history page displays the user's username; a link to the user's contributions; and a link to his "User page." That history of the user's contributions and edits is also available via a "Special: Contributions" link from the User page.

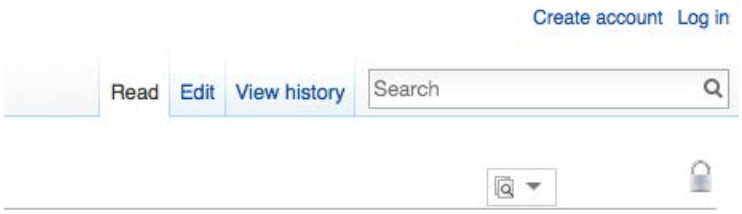
Figure 3



B. Searching and Navigating Wikipedia

17. As shown in Figure 4, users may search Wikipedia by entering a search term; on the desktop version of the site, shown here, the search box is located in the upper-right corner of the screen.

Figure 4



18. Where the search identifies a Wikipedia page with a title that corresponds exactly to the search team, the user is sent directly to that page. The URL of the resulting page incorporates the relevant topic and reveals information about the content of the requested page. For example, when a user employs a search for "substance abuse," the resulting webpage URL is https://en.wikipedia.org/wiki/Substance_abuse.

19. When a search does not identify a Wikipedia page with a title that corresponds exactly to the search team, the user is sent directly to a "Search results" page. The URL of the search results page incorporates the search term employed by that user. For example, if a user searches for "Kansas City Monsoon"—a fictional event with no corresponding Wikipedia page—he would be directed to a Search results page with the following URL: https://en.wikipedia.org/w/index.php?search=Kansas+City+Monsoon&title=Special%3ASearch&go=Go.

20. Additionally, Wikipedia pages include links to other Wikipedia pages on related topics that enable the reader to access those pages directly from the page being viewed. For instance, the Wikipedia page on "Substance abuse" references "anti-social behavior," and includes

a link to the Wikipedia page on this topic, http://en.wikipedia.org/wiki/Anti-social_behaviour.

21. In 2017, Wikimedia sites received over 237 billion page views, with approximately 74 billion views originating from users in the United States.

C. User Discussions

22. Wikimedia also engages in communications that permit its users to interact with one another more directly. Wikimedia Project pages feature "Talk" pages (also known as "Discussion" pages) in which users can publicly discuss potential changes to an article or other Wikimedia Project page. When viewing a Wikimedia Project page on the desktop version of the site, the link to the corresponding Talk page appears on the top left of the screen. A depiction of a Talk page tab and an article Talk page is shown in Figures 5 and 6 below.

Figure 5

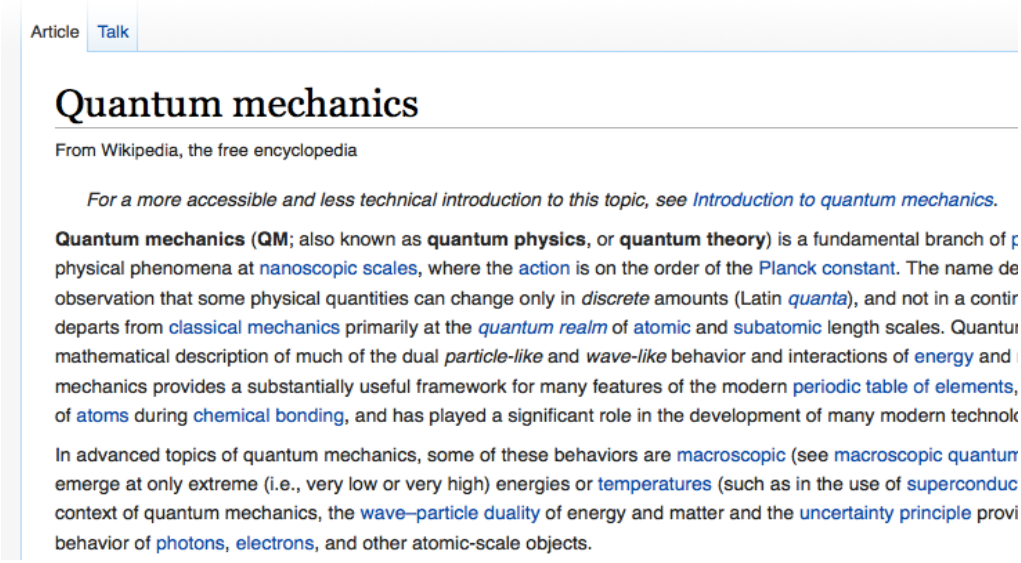
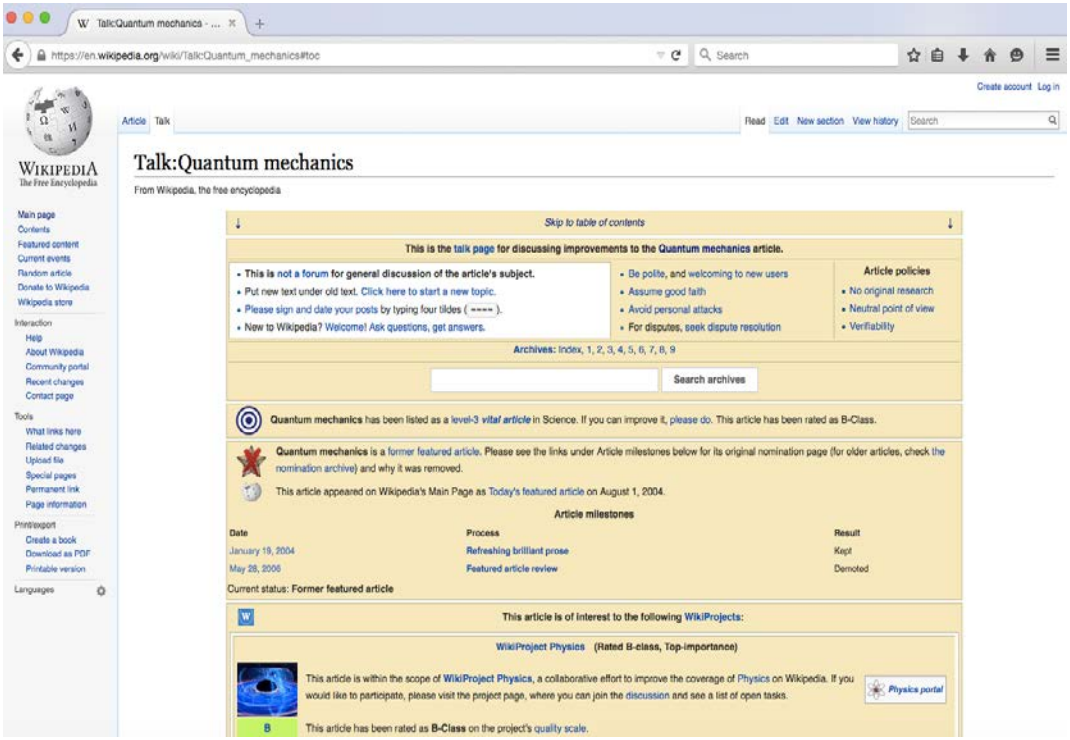
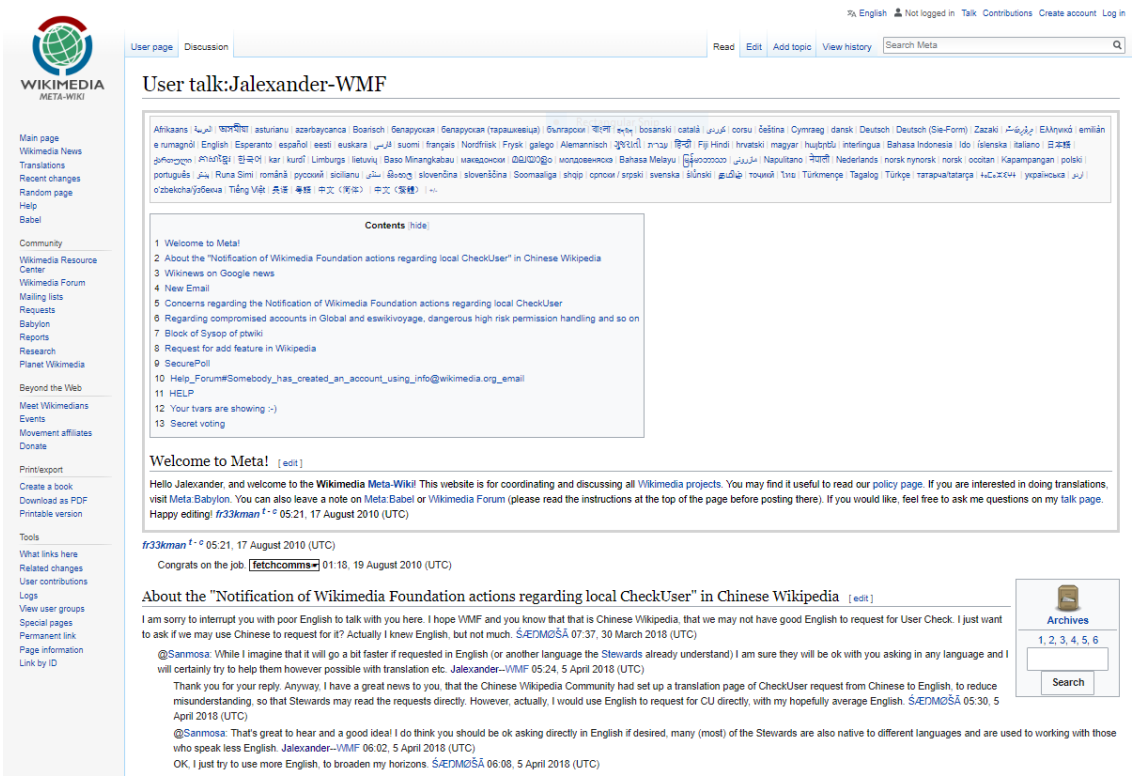


Figure 6



23. User pages also have associated Talk pages. One user may contact another by leaving a message on his Talk page. As with edits, Talk page comments are publicly visible and associated with the commenter's username, or, if the user is commenting without logging in, the user's IP address. Figure 7 illustrates a user's Talk page.

Figure 7



24. Users may also interact with one another and with Wikimedia using private or semi-private communication features on Project websites. The primary examples of these features are discussed below.

- *OTRS*. The Open-source Ticket Request System is a software package employed by Wikimedia since 2004 to address queries, complaints, and comments about the Wikimedia Projects from users. Responses are handled primarily by a group of trusted Wikimedia users who volunteer to answer these queries, complaints, and comments, and certain responses are handled by Wikimedia staff. In other words, OTRS messages are private communications between Wikimedia users or between users and Wikimedia staff.

- *Email User Feature*. This feature allows registered users to exchange emails with one another via Wikimedia, provided that both users have enabled email communications on their Wikimedia accounts. For example, a Wikimedia user can send an email to another Wikimedia user's Gmail account by visiting the intended recipient's User page and selecting an email option. The content of the communication is entered into an HTML form and transferred via HTTPS to Wikimedia servers, and from there to the recipient's email address using the standard SMTP email protocol.

- *Private Mailing Lists.* Users may create or be invited to use "private mailing lists" through Wikimedia. Users must seek permission from the mailing list administrator to receive access to, send, or receive emails through the list, and to read historical archives of mail sent to the list. List messages are sent and received using the SMTP protocol, while archives are accessed via HTTP/S (both via Wikimedia's servers at lists.wikimedia.org). For example, Wikimedia Israel Galleries, Libraries, Archives and Museums coordination is one such private mailing list: https://lists.wikimedia.org/mailman/listinfo/wikimedia-il-glam.

- *Private Wikis.* Some groups of users, for example OTRS volunteers, also employ "private wikis" to communicate about specific topics. These wikis are only accessible by certain users. Wikimedia servers host these communications, which are transmitted via HTTP/S.

III. STATISTICS ON WIKIMEDIA'S INTERNATIONAL INTERNET COMMUNICATIONS

25. As the operator of one of the most-visited websites in the world, Wikimedia engages in an extraordinarily high volume of Internet communications with individual users located around the globe, some of whom are Americans located abroad. *See*, *e.g.*, Exhibit 10 (WIKI0009221, -9222) (American citizen and Wikimedia user located abroad requesting ability to use web application designed to anonymize online activity). Indeed, its servers handle more than one trillion international communications each year, with individuals who are located in every country on earth.

26. Wikimedia's international communications can be divided into the following three categories, each of which contain sensitive and private information related to Wikimedia and its users:

- **Category 1 – *Wikimedia communications with its community members***. Examples of these communications include, but are not limited to, page views to Wikimedia websites, edits and contributions to Wikimedia websites, emails between registered Wikimedia users and emails on Wikimedia's mailing lists. The vast majority of these communications are generated by HTTP and HTTPS requests from users who read and contribute to Wikimedia's Projects, and who use the Projects and webpages to interact with each other.

- **Category 2 – *Wikimedia's internal log communications*.** Wikimedia maintains proprietary "logs" that catalogue a variety of information regarding each HTTP or HTTPS request to a Wikimedia resource. These logs help Wikimedia monitor, study, and improve the Projects. Every time Wikimedia receives an HTTP or HTTPS request from a person

accessing a Project webpage, it creates a corresponding log entry. Depending on the location of the user and the routing of that user's request, the log may be generated by Wikimedia's servers abroad, which in turn send the log entry to Wikimedia in the United States. Wikimedia also uses information about the log communications to inform its site operations, improve user interfaces, and to guide support work for its volunteer community.

- **Category 3 – *Wikimedia's staff communications.*** Wikimedia's office network router located in the United States also handles a variety of border-crossing communications. Examples of these communications include, but are not limited to, Gmail, Google chat, Internet Relay Chat, and Slack. Additionally, Wikimedia staff members use a variety of third-party tools to conduct their work, including, but not limited to, Google Apps/G Suite, Trello, Sugar, Qualtrics, UserTesting and Salesforce. Wikimedia's staff communications reveal a variety of highly sensitive information about Wikimedia's operations, and include communications with international staff who are involved in political or social activism and live or work in geopolitical areas that are a special focus of the U.S. government's counterterrorism or diplomatic efforts.

27. Wikimedia is able to use its server log data to quantify each of these categories of international communications by Internet protocol and country of origin. I led the process of calculating these communications volume figures in response to Defendants' written discovery requests. The results of these analyses are contained in Wikimedia's Exhibit 14 and described below:

Category 1 Volume – *Wikimedia communications with its community members*

- Total HTTP and HTTPS requests from foreign users to Wikimedia's U.S. servers: Between August 1, 2017 and January 31, 2018, Wikimedia's U.S. servers received approximately **381 billion HTTP/S requests** from users outside of the United States. Wikimedia calculated this figure using MaxMind[2] geolocation data to determine the country associated with the client IP of each HTTP/S request transmitted to Wikimedia's servers in the United States.

- Total HTTP and HTTPS requests from U.S. users to Wikimedia's foreign servers: Between August 1, 2017 and January 31, 2018, Wikimedia's foreign-based servers received approximately **2.8 billion HTTP/S requests** from users in the United States. Wikimedia calculated this figure using MaxMind geolocation data to determine the country associated with the client IP of each HTTP/S request transmitted to Wikimedia's servers located outside the United States.

[2] MaxMind is a U.S.-based company that provides widely used databases for Internet geolocation.

Category 2 Volume – *Wikimedia's internal log communications*

- Total log communications transmitted from Wikimedia's foreign servers to Wikimedia's U.S. servers: Between August 1, 2017 and January 31, 2018, Wikimedia's foreign-based servers transmitted approximately **736 billion log communications** to Wikimedia servers in the United States, using the Apache Kafka protocol. These communications were encrypted using IPsec, a secure network protocol suite that authenticates and encrypts the packets of data sent over a network.

Category 3 Volume – *Communications by Wikimedia staff*

- Total logged international TCP connections using Wikimedia's office network or VPN: Between March 1, 2017 and February 28, 2018, Wikimedia's office network router located in the United States logged open Internet connections using the Transmission Control Protocol (TCP) with non-U.S. countries, territories and regions at least approximately **4,948,011** times.

- Total logged international UDP connections using Wikimedia's office network or VPN: Between March 1, 2017 and February 28, 2018, Wikimedia's office network router located in the United States logged open Internet connections using the User Datagram Protocol (UDP) with non-U.S. countries, territories and regions at least approximately **2,207,771** times.

- Total logged international ICMP connections using Wikimedia's office network or VPN: Between March 1, 2017 and February 28, 2018, Wikimedia's office network router located in the United States logged open Internet connections using the Internet Control Message Protocol (ICMP) with non-U.S. countries, territories and regions at least approximately **51,301** times.

28. Wikimedia calculated the Category 3 communications using MaxMind geolocation data to determine the country associated with the source and destination IPs of each of these Internet connections. The router generated a log of all open Internet connections, including their protocol and source and destination IPs, every five minutes, using a program called "conntrack." Connections that remained open for more than five minutes may have been logged more than one time. Connections that remained open for less than five minutes may not been logged at all. These figures include, but are not limited to, connections sent through Wikimedia's virtual private network (VPN), which passed through the same router and can be distinguished in the log by the IP address used to connect.

29. In response to discovery requests in this litigation, I also quantified and verified other statistics relevant to the volume of Wikimedia's communications, a subset of which are contained below in Figure 8.

Figure 8

Wikimedia Statistics and Volume Metrics

	Number	Date Range
Wikipedia articles	47,433,067	As of February 9, 2018
Wikipedia languages	288	As of February 9, 2018
Edits over the lifespan of the Wikimedia Projects	approx. 3.4 billion	As of February 28, 2018
Range of monthly unique devices visiting Wikipedia pages	1,521,315,531 (high) / 1,361,541,637 (low)	High/low range for April 2017 to December 2017
Range of monthly U.S. unique devices visiting Wikipedia pages	284,472,345 (high) / 261,065,481 (low)	High/low range for April 2017 to December 2017
Page views	237,586,909,120	January 1, 2017 to December 31, 2017 (one year)
U.S. page views	74,182,143,412	January 1, 2017 to December 31, 2017 (one year)

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on December 19, 2018 in Sindelfingen, Germany.

Tilman Bayer

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 6

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, *Plaintiff*, v. NATIONAL SECURITY AGENCY / CENTRAL SECURITY SERVICE, *et al.*, *Defendants*.	No. 1:15-cv-00662-TSE

DECLARATION OF EMILY TEMPLE-WOOD

I, Emily Temple-Wood, declare:

1. I am a resident of Downers Grove, Illinois, over the age of eighteen. I have personal knowledge of the facts stated in this declaration, and, if called to testify, I could and would testify competently thereto. I am providing this declaration in my capacity as a Wikimedia Foundation, Inc. ("Wikimedia") community member. I am not an employee or contractor of Wikimedia.

2. I completed a Bachelor of Science degree from Loyola University Chicago, and I am currently a third-year medical student at Chicago College of Osteopathic Medicine at Midwestern University.

I. Background

3. Wikimedia is a nonprofit charitable organization based in San Francisco, California, dedicated to encouraging the growth, development, and distribution of multilingual educational content, and to providing the full content of "wiki"-based projects to the public free of charge.

Wikimedia operates twelve free-knowledge projects ("Projects") on the Internet, including Wikipedia, the world's largest and most popular encyclopedia.

4. I have been a member of the Wikimedia community—as a reader and an editor—for more than 11 years. Since April 2007, I have served as an editor of the English Wikipedia. As an editor, I create original articles for Wikipedia, add original content to existing Wikipedia articles, and edit others' content for accuracy and compliance with Wikipedia's principles, including adherence to a neutral point of view. I have created nearly 400 articles on Wikipedia and have edited thousands more, on topics ranging from biology to women scientists.

5. I have also held several leadership positions within the Wikimedia community. Since November 2007, I have served as an English Wikipedia administrator. Administrators are community leaders, appointed by other community members, who help maintain the integrity of Wikipedia's content. Administrators' responsibilities include blocking certain disruptive users from editing the site, protecting articles from vandalism, deleting and undeleting Wikipedia articles, and mediating disputes.

6. From January 2016 through December 2017, I served on the English Wikipedia's Arbitration Committee. Arbitrators are elected directly by the English Wikipedia community and resolve community disputes over Wikipedia users' conduct when all other dispute-resolution mechanisms have failed. The Committee is also empowered to penalize and ban members who misuse administrative privileges or who are disruptive to the functioning of the community. In addition, the Committee issues binding judgments on matters of Wikipedia policy and clarifies the principles of Wikipedia's governance.

7. Since the summer of 2015, I have served as a Wikipedia Oversighter. Oversighters are appointed after review by the English Wikipedia community and the Arbitration Committee.

Oversighters' responsibilities include removing non-public personal information that is improperly posted to Wikipedia's public webpages, such as phone numbers, addresses, and identities of anonymous users; removing libel and defamatory content; and removing content that infringes copyrights.

II. Relationship Between Wikimedia and Its Users

8. The relationship between Wikimedia and its community of users is so close and intertwined that it is symbiotic: one cannot exist without the other. Users rely on Wikimedia's administrative and technical expertise to create, edit, distribute, and receive free educational content, and Wikimedia relies on its users to create, edit, distribute, and receive that content in furtherance of its mission. Volunteers play critical roles that keep the Projects functioning, such as the administrator, arbitrator, and oversighter roles described above.

9. Wikimedia supports its user community in myriad ways. For one, it operates and provides the technical infrastructure for the Wikimedia Projects, including Wikipedia. It also administers grants to benefit the Wikimedia community and movement, develops software for the community, and works with community members to organize conferences and community-outreach events around the world.

10. Like many other members of the Wikimedia community, I have worked closely with Wikimedia staff. Specifically, my work as an administrator, arbitrator, and oversighter has required extensive communication with Wikimedia staff. In addition, in both 2014 and 2015, I applied for and received grants of $7,000 from Wikimedia to help engage more women as Wikipedia editors. These grants enabled me to develop techniques for recruiting and retaining women editors. Over the course of several years, I also applied for and received scholarships from Wikimedia to attend ten conferences with Wikimedia staff and users.

11. Wikimedia exists to facilitate the user community's work in fulfilling the shared mission of the Wikimedia movement, and the user community would quickly collapse without Wikimedia's infrastructure, network, and support. Wikimedia and its community members depend on one another in pursuit of their shared goal of ensuring that knowledge is free.

III. The Importance of Wikimedia's Non-U.S. Readers and Contributors to U.S. Users

12. My interest in contributing to Wikipedia is based in part on my ability to reach an international audience. Free information is not just for Americans—it is for everyone. Indeed, the very purpose of Wikipedia is to create and distribute the largest and most comprehensive encyclopedia ever written—one of the highest possible quality, that is available for free to every single person on the planet in his or her own language. My contributions to Wikipedia are in furtherance of this mission and of my belief that information on Wikipedia should be freely available to U.S. and non-U.S. persons alike.[1] These contributions have been read by Wikipedia users abroad.

13. I also read and benefit from the contributions of non-U.S. users on a wide array of topics, such as biographies of notable women from around the world, films, history, astronomy, rare diseases, anatomy, and pathology. Wikipedia seeks to amass the sum of human knowledge, and that is simply impossible without the voices of foreign contributors located abroad.

14. Wikimedia community members are spread around the world. As a Wikimedia community member, my relationship with non-U.S. users is crucial to my involvement with Wikimedia.

[1] In this context, by "non-U.S. persons," I mean individuals who are located outside the United States.

15. For example, I interact with and rely on non-U.S. Wikimedia users through the Wikipedia project "Women in Red."[2] This project is designed to address the fact that a disproportionate number of biographies on Wikipedia concern the lives of notable men. Seeking to remedy this gender gap, Women in Red encourages Wikipedia users to create and contribute to articles discussing the biographies and works of notable women. The project has resulted in articles in dozens of languages, including English, Farsi, Catalan, German, Greek, Spanish, French, Italian, Hebrew, Dutch, Albanian, Tamil, Thai, Ukrainian, and Mandarin. As a result of Women in Red, I have read and benefitted from the contributions of many non-U.S. Wikimedia community members to English-language biographies of women.

16. I also deeply value my relationships with the non-U.S. Wikimedia users I have met through Wikimedia conferences. The largest annual conference for the Wikimedia movement, known as "Wikimania," takes place in a new international location each year. The purpose of the conference is to bring together community members from around the world for discussions, trainings, and exchanges of ideas. I have attended four of these conferences, where I have met hundreds of members of the global Wikimedia community.

17. After the conferences, I have continued to communicate with many non-U.S. Wikimedia community members through various means, including Wikipedia "Talk" pages, user "Talk" pages, and private email lists organized by Wikimedia.[3] For example, at the 2013 Wikimania conference in Hong Kong, I had lengthy discussions with my roommate for the week—a Wikipedia contributor from Iraq—about gaps in Wikipedia content. At the conference, I gave a talk about missing women scientists' content, and non-U.S. attendees encouraged me to

[2] *See* https://en.wikipedia.org/wiki/Wikipedia:WikiProject_Women_in_Red.

[3] These pages, also known as "discussion" pages, allow users to publicly discuss potential changes to an article or other Wikimedia Project page.

focus on remedying this gap. After the conference concluded and we returned to our respective countries, we continued these discussions online through Wikipedia pages, which led to the founding of "WikiProject Women Scientists."[4] These conversations inspired me to create and develop dozens of biographies of women scientists on Wikipedia—work that helped deepen my ties to the Wikimedia community, and which led to my being named "Wikimedian of the Year" in 2016.

IV. Importance of Anonymity to Wikimedia Users

18. Anonymity is essential to the Wikimedia user community, including individuals who read or edit Wikimedia Project pages.

19. Although some of my Wikipedia contributions are publicly linked to my real-world identity, I also contribute to Wikipedia under a separate, pseudonymous account when writing about especially sensitive topics. As a medical student, I have a professional interest in gynecology, pediatric gynecology, abortion care, sexually transmitted infections, and LGBTQ health. As a Wikipedia reader, I have accessed Wikipedia pages concerning these issues. As a Wikimedia editor, in order to advance others' understanding of these topics, I have pseudonymously posted images of myself that depict gynecological anatomy and pathology. Given the extremely sensitive nature of these topics, it is essential that I am able to read and contribute to Wikipedia anonymously. When I read and contribute to Wikipedia anonymously, I consider information connecting my identity to the pages I have read or the contributions I have made on Wikipedia to be private.

20. As a Wikipedia user, I am concerned about government surveillance, including Upstream surveillance of my communications with Wikimedia servers located abroad.

[4] *See* https://en.wikipedia.org/wiki/Wikipedia:WikiProject_Women_scientists.

21. Anonymity is critical to non-U.S. Wikimedia users as well. Over the years, I have worked with numerous members of the Wikimedia community who did not disclose their identities because anonymity was so important to them, including Wikipedia administrators, contributors to Women in Red, and users who peer-review articles to ensure that they meet Wikipedia's standards for content quality. Because these users were anonymous, I cannot be certain of their nationality. However, given that some were non-native English speakers, I believe that at least some of these Wikimedia users are non-U.S. persons.

22. Some non-U.S. Wikimedia users have contributed anonymously to Wikimedia about controversial current events in their home countries, because they face grave repercussions if their identities are linked to their online activity. A notable example is an anonymous Wikimedia contributor based in Venezuela. This user posted photographs of anti-government protests in Venezuela to Wikimedia Commons, an online database of media files available for free use. The Venezuelan government eventually uncovered this user's identity and revoked his passport as a result of his contributions to Wikimedia.[5]

23. Upstream surveillance threatens the anonymity and privacy of individuals who visit the Wikimedia Projects. Because of this, and based on my conversations with foreign Wikimedia users living in countries such as Iraq, the United Kingdom, New Zealand, and Singapore, I believe that it is very likely that NSA surveillance has resulted and will result in some foreign readers, editors, contributors, and volunteers being less willing to read, contribute to, or otherwise engage with the Projects, because they fear that their communications will be

[5] Joe Sutherland, *2015 Wikipedians of the Year Unveiled in Mexico*, Wikimedia Blog (July 31, 2015), https://blog.wikimedia.org/2015/07/31/wikipedians-of-the-year-2015/.

intercepted by the U.S. government and also shared with other governments, intelligence services, and organizations with which the U.S. cooperates.

24. In sum, NSA surveillance, including Upstream surveillance, threatens the privacy and anonymity of foreign and domestic members of the Wikimedia community, and that threat discourages individuals from engaging with the Wikimedia Projects.

V. Obstacles to Filing Suit

25. The impact of Upstream surveillance is spread across millions of Wikimedia users and contributors around the world, some of whom may use the Projects a great deal and others who may access the body of knowledge that Wikimedia provides only intermittently. In this context, the obstacles and disincentives that any particular user faces in bringing suit as an individual are significant.

26. First, given the amount of time and resources necessary to pursue a federal lawsuit, as well as the legal and technical complexity of a case challenging the NSA's surveillance practices, I lack the capacity to bring a lawsuit challenging Upstream surveillance on my own behalf. My workload as a medical student would make such a suit impossible. Many Wikimedia community members, including myself, contribute to Wikimedia Projects in their scarce free time, alongside their responsibilities as students, wage-earners, and/or family caretakers.

27. Second, and as importantly, serving as a plaintiff in a lawsuit would threaten the anonymity that users depend on when reading and contributing to the Wikimedia Projects. For example, given the sensitive nature of the articles I read and contribute to on Wikipedia, as summarized above, I would face substantial personal consequences if they were disclosed and dissected in detail in the course of litigation, including through the discovery process.

28. Finally, I fear that if I were to bring a lawsuit challenging U.S. government surveillance, I would risk subjecting myself to unwarranted scrutiny from the U.S. government.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on December 17, 2018 in Downers Grove, Illinois.

Emily Temple-Wood

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 7

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, *Plaintiff*, v. NATIONAL SECURITY AGENCY / CENTRAL SECURITY SERVICE, *et al.*, *Defendants*.	Hon. T. S. Ellis, III Civil Action No. 15-cv-00662-TSE

DECLARATION OF PATRICK TOOMEY IN SUPPORT OF PLAINTIFF WIKIMEDIA FOUNDATION'S OPPOSITION TO DEFENDANTS' MOTION FOR SUMMARY JUDGMENT

I, Patrick Toomey, a member of the Bar of the State of New York and admitted *pro hac vice* to the Bar of this Court, declare under penalty of perjury as follows:

1. I am an attorney with the American Civil Liberties Union Foundation, and represent Plaintiff Wikimedia Foundation ("Wikimedia") in this matter. I submit this declaration in support of Plaintiff Wikimedia's Opposition to Defendants' Motion for Summary Judgment (ECF No. 161).

2. Filed as Exhibits 1-45 attached to Plaintiff's Opposition to Defendants' Motion for Summary Judgment are true and correct copies of the following documents:

No.	Exhibit
1	Declaration of Scott Bradner and attached Appendix
2	Declaration of Jonathon Penney and attached Appendix
3	Declaration of Michelle Paulson
4	Declaration of James Alexander

5	Declaration of Tilman Bayer
6	Declaration of Emily Temple-Wood
7	Declaration of Patrick Toomey
8	Wikimedia-hosted email list discussing NSA slide with Wikimedia logo, from July to August 2013
9	Wikimedia "Talk page" discussing its non-public information policy, from September to December 2013
10	"OTRS" ticket showing Wikimedia user requesting Tor permissions in September 2013[1]
11	Wikimedia webpage showing Wikimedia user requesting Tor permissions in September 2017
12	Wikimedia document compiling German-user-community appeal concerning privacy in 2013
13	Wikimedia "Talk page" discussing NSA surveillance from June to December 2013
14	Wikimedia Technical Statistics Chart & Supporting Exhibits A-G
15	Privacy & Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of FISA* (July 2014)
16	FISC Memorandum Opinion, [*Redacted*], 2011 WL 10945618 (Oct. 3, 2011)
17	Office of the Director of National Intelligence, *DNI Declassifies Intelligence Community Documents Regarding Collection Under Section 702 of FISA* (Aug. 21, 2013), http://icontherecord.tumblr.com/post/58944252298/dni-declassifies-intelligence-community-documents
18	Defendant NSA's Objections and Responses to Plaintiff's First Set of lnterrogatories (Dec. 22, 2017)
19	FISC Submission, *Clarification of National Security Agency's Upstream Collection Pursuant to Section 702 of FISA* (May 2, 2011)
20	Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities, Calendar Year*

[1] This document is a true and correct version of the "OTRS" ticket with certain identifying information redacted, as produced to Defendants in discovery.

	2017 (Apr. 2018), https://www.dni.gov/files/documents/icotr/2018-ASTR----CY2017----FINAL-for-Release-5.4.18.pdf
21	FISC Memorandum Opinion & Order (Apr. 26, 2017)
22	FISC Submission, *Government's Response to the Court's Briefing Order of May 9, 2011* (June 1, 2011)
23	*Big Brother Watch & Others v. United Kingdom*, App. Nos. 58170/13, 62322/14, 24960/15, Eur. Ct. H.R. (2018)
24	NSA Director of Civil Liberties & Privacy Office, *NSA's Implementation of FISA Section 702* (Apr. 16, 2014)
25	*Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection System (EINSTEIN 2.0)*, 33 Op. O.L.C. 1 (Jan. 9, 2009)
26	Minimization Procedures Used by the NSA in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of FISA (July 2014)
27	Glenn Greenwald, *XKeyscore: NSA Tool Collects "Nearly Everything a User Does on the Internet"*, Guardian, July 31, 2013, https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data
28	NSA slide, excerpted from Exhibit 27 (Greenwald, *XKeyscore: NSA Tool Collects "Nearly Everything a User Does on the Internet"*)
29	Morgan Marquis-Boire, *et al.*, *XKEYSCORE: NSA's Google for the World's Private Communications*, Intercept, July 1, 2015, https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications
30	NSA slide deck, *XKEYSCORE for Counter-CNE*, published in The Intercept on July 1, 2015, https://theintercept.com/document/2015/07/01/xks-counter-cne
31	Wikimedia, *Founding Principles* (accessed Mar. 14, 2018)
32	Yana Welinder, *Opposing Mass Surveillance on the Internet*, Wikimedia Blog (May 9, 2014), https://blog.wikimedia.org/2014/05/09/opposing-mass-surveillance-on-the-internet
33	Wikimedia Public Policy, *Privacy* (accessed Mar. 14, 2018)

34	Wikipedia, *Sock Puppetry* (accessed Mar. 14, 2018)
35	Wikimedia, *Privacy Policy* (accessed Feb. 14, 2018)
36	Ryan Lane, *The Future of HTTPS on Wikimedia Projects*, Wikimedia Blog (Aug. 1, 2013), http://blog.wikimedia.org/2013/08/01/future-https-wikimedia-projects
37	Yana Welinder, *et al.*, *Securing Access to Wikimedia Sites with HTTPS*, Wikimedia Blog (June 12, 2015), http://blog.wikimedia.org/2015/06/12/securing-wikimedia-sites-with-https
38	Wikimedia email describing Tech/Ops goals and the importance of HTTPS (May 23, 2014)
39	Wikimedia document discussing IPsec implementation, including July 8, 2013 statement from a Wikimedia engineer
40	Wikimedia job posting for Traffic Security Engineer (accessed Feb. 8, 2018)
41	Michelle Paulson, *A Proposal for Wikimedia's New Privacy Policy and Data Retention Guidelines*, Wikimedia Blog (Feb. 14, 2014), https://blog.wikimedia.org/2014/02/14/a-proposal-for-wikimedias-new-privacy-policy
42	Wikimedia's Supplemental Exhibit C in response to NSA Interrogatory No. 8 (volume of HTTP border-crossing communications by country)
43	Wikimedia's Supplemental Exhibit D in response to NSA Interrogatory No. 8 (volume of HTTPS border-crossing communications by country)
44	Wikimedia analytics document showing monthly unique visitors to Wikimedia by region, from December 2007 to May 2015
45	Press Release, NSA, *NSA Stops Certain Section 702 "Upstream" Activities*, Apr. 28, 2017, https://www.nsa.gov/news-features/press-room/Article/1618699/nsa-stops-certain-section-702-upstream-activities

* * *

I declare under penalty of perjury that the foregoing is true and correct.

Patrick Toomey

Date: December 18, 2018
New York, New York

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 8

Re: [Wikimedia-l] NSA [In reply to]

fredbaud at fairpoint

Jul 31, 2013, 6:28 PM
Post #26 of 45 (2064 views)
Permalink

I think it's more reasonable to assume that
> Wikipedia (which shares many features with Google, Yahoo, Twitter, Facebook and other social networks) has been the subject of this kind of demand than that it hasn't. No one with direct knowledge would be able to do anything other than deny it, but we can easily see why data held by Wikipedia (including partially anonymized e-mails, file
> uploads, talk page communication, etc.) would be of interest to
> intelligence agencies.

The capacity of the Wikimedia Foundation to keep a secret of this nature
is low. Simply too many outlaws; something NSA could probably figure out;
they are not called intelligence for nothing.

Fred

Changed "law" to "low"

Wikimedia-l mailing list
Wikimedia-l@lists.wikimedia.org
Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Re: [Wikimedia-l] NSA [In reply to]

marc at uberbox

Jul 31, 2013, 6:59 PM
Post #27 of 45 (2051 views)
Permalink

On 07/31/2013 09:27 PM, Ryan Lane wrote:
> I would be fired and jailed before I knowingly let that occur. If this was
> the case I'd very surely not be working for Wikimedia Foundation.

And very many of us live outside the jurisdiction of the entities that would be doing the monitoring and would be very noisy indeed if something of that nature took place.

-- Marc

Re: [Wikimedia-l] NSA [In reply to]

marc at uberbox

Jul 31, 2013, 7:06 PM
Post #28 of 45 (2050 views)
Permalink

On 07/31/2013 07:52 PM, Nathan wrote:
> If anything, I think it's more reasonable to assume that
> Wikipedia (which shares many features with Google, Yahoo, Twitter,
> Facebook and other social networks) has been the subject of this kind
> of demand than that it hasn't.

You're also making an unwarranted leap there: that the Foundation would
comply with such a demand, if one was made, rather than fight it tooth and nail. In fact, the WMF probably has acquired quite a reputation amongst intelligence circles as being quire uncooperative when it comes
to stomping faces with boots.

There are very few people who work for an organization that has as its primary objective the free dissemination of knowledge that wouldn't be willing to rattle the cages of those who seek to suppress it. If nothing else, we are very good at pointing out egg on faces in a very public, very visible way.

-- Marc

Re: [Wikimedia-l] NSA [In reply to]

toddmallen at gmail

Jul 31, 2013, 7:11 PM

Also keep in mind that WMF has explicitly stated that they received no such
demand. If they had, they still could say "If we had received such a

demand, we couldn't legally discuss it", still comply with the order, and let us read between the lines. While I don't always agree with WMF, I have
more regard for them than to think they would flat out lie about a matter that important.
On Jul 31, 2013 7:59 PM, "Marc A. Pelletier" <marc@uberbox.org> wrote:

> On 07/31/2013 09:27 PM, Ryan Lane wrote:
> > I would be fired and jailed before I knowingly let that occur. If this
> was
> > the case I'd very surely not be working for Wikimedia Foundation.
>
> And very many of us live outside the jurisdiction of the entities that
> would be doing the monitoring and would be very noisy indeed if
> something of that nature took place.
>
> -- Marc
>
>
> _____
> Wikimedia-l mailing list
> Wikimedia-l@lists.wikimedia.org
> Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
> <mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

_____
Wikimedia-l mailing list
Wikimedia-l@lists.wikimedia.org
Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Re: [Wikimedia-l] NSA [In reply to]

jsalsman at gmail

Jul 31, 2013, 7:51 PM
Post #30 of 45 (2056 views)
Permalink

Nathan wrote:
>
>... It seems that most of the data they
> collect is wiped within 3 days; that the data itself can only be
> analyzed under a fairly specific set of minimization rules....

Are you referring to the 2009 Holder minimization rules which per http://m.newyorker.com/online/blogs/closeread/2013/06/how-many-americans-does-the-nsa-spy-on-a-lot-of-them.htmlrequire sharing records on anyone who has ever sent or received email or chat from a foreign national with the FBI, or the more recent "three hop"

minimization rules which require permanent storage of the records pertaining to the roughly one billion people who are connected to people connected to people connected with suspects?

Re: [Wikimedia-l] NSA [In reply to]

wikimail at inbox

Jul 31, 2013, 9:15 PM
Post #31 of 45 (2051 views)
Permalink

On Wed, Jul 31, 2013 at 9:27 PM, Ryan Lane <rlane@wikimedia.org> wrote:

> I would be fired and jailed before I knowingly let that occur. If this was
> the case I'd very surely not be working for Wikimedia Foundation.
>

Key word there being "knowingly".

Re: [Wikimedia-l] NSA [In reply to]

tstarling at wikimedia

Jul 31, 2013, 9:44 PM
Post #32 of 45 (2052 views)
Permalink

On 01/08/13 14:15, Anthony wrote:
> On Wed, Jul 31, 2013 at 9:27 PM, Ryan Lane <rlane@wikimedia.org> wrote:
>
>> I would be fired and jailed before I knowingly let that occur. If this was
>> the case I'd very surely not be working for Wikimedia Foundation.
>>
>
> Key word there being "knowingly".

I don't know why the NSA would sneak around in our data centres mirroring our ethernet ports if they already have almost all of our access logs by capturing unencrypted traffic as it passes through XKeyscore nodes.

I think you should save the conspiracy theories until after we switch

anons to HTTPS, that's when they will have an incentive.

-- Tim Starling

Re: [Wikimedia-l] NSA [In reply to]

akoval at wikimedia

Jul 31, 2013, 10:36 PM
Post #33 of 45 (2051 views)
Permalink

very helpful, james. thanks so much for clue-ing me in. definitely want to know more of the backstory on the chapters sometime. ttyt :)

On Wednesday, July 31, 2013, Tim Starling wrote:

> On 01/08/13 14:15, Anthony wrote:
> > On Wed, Jul 31, 2013 at 9:27 PM, Ryan Lane
<rlane@wikimedia.org<javascript:;>>
> wrote:
> >
> >> I would be fired and jailed before I knowingly let that occur. If this
> was
> >> the case I'd very surely not be working for Wikimedia Foundation.
> >>
> >
> > Key word there being "knowingly".
>
> I don't know why the NSA would sneak around in our data centres
> mirroring our ethernet ports if they already have almost all of our
> access logs by capturing unencrypted traffic as it passes through
> XKeyscore nodes.
>
> I think you should save the conspiracy theories until after we switch
> anons to HTTPS, that's when they will have an incentive.
>
> -- Tim Starling
>
>
> _____
> Wikimedia-l mailing list
> Wikimedia-l@lists.wikimedia.org <javascript:;>
> Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,

--
Anna Koval
Community Advocate
Wikimedia Foundation
415-839-6885 x 6729
akoval@wikimedia.org

Wikimedia-l mailing list
Wikimedia-l@lists.wikimedia.org
Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Re: [Wikimedia-l] NSA [In reply to]

akoval at wikimedia

Jul 31, 2013, 10:48 PM
Post #34 of 45 (2060 views)
Permalink

Whoops! :) That wasn't meant to be a reply-to-all. Sorry, everyone.
Rookie
mistake... :]

On Wed, Jul 31, 2013 at 10:36 PM, Anna Koval
<akoval@wikimedia.org> wrote:

> very helpful, james. thanks so much for clue-ing me in. definitely want
> to know more of the backstory on the chapters sometime. ttyt :)
>
>
> On Wednesday, July 31, 2013, Tim Starling wrote:
>
>> On 01/08/13 14:15, Anthony wrote:
>> > On Wed, Jul 31, 2013 at 9:27 PM, Ryan Lane
<rlane@wikimedia.org> wrote:
>> >
>> >> I would be fired and jailed before I knowingly let that occur. If this
>> was
>> >> the case I'd very surely not be working for Wikimedia Foundation.
>> >>
>> >
>> > Key word there being "knowingly".
>> >
>> I don't know why the NSA would sneak around in our data centres

>> mirroring our ethernet ports if they already have almost all of our
>> access logs by capturing unencrypted traffic as it passes through
>> XKeyscore nodes.
>>
>> I think you should save the conspiracy theories until after we switch
>> anons to HTTPS, that's when they will have an incentive.
>>
>> -- Tim Starling
>>
>>
>> _____
>> Wikimedia-l mailing list
>> Wikimedia-l@lists.wikimedia.org
>> Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
>> <mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>
>
>
>
> --
> *Anna Koval*
> Community Advocate
> Wikimedia Foundation
> 415-839-6885 x 6729
> akoval@wikimedia.org
>
>

--
Anna Koval
Community Advocate
Wikimedia Foundation
415-839-6885 x 6729
akoval@wikimedia.org

_____
Wikimedia-l mailing list
Wikimedia-l@lists.wikimedia.org
Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Re: [Wikimedia-l] NSA [In reply to]

No, but presenting an appearance of surprise is a bit disingenuous.
P

peter.southwood at telkomsa

Post #35 of 45 (2048 views)

Permalink

----- Original Message -----
From: "David Gerard" <dgerard@gmail.com>
To: "Wikimedia Mailing List" <wikimedia-l@lists.wikimedia.org>
Sent: Wednesday, July 31, 2013 11:10 PM
Subject: Re: [Wikimedia-l] NSA

> On 31 July 2013 21:47, Ryan Lane <rlane@wikimedia.org> wrote:
>
>> Why would we expect that we weren't being targeted? Knowing what people
>> are
>> looking up is powerful knowledge.
>
>
> That doesn't make it one dot less reprehensible.
>
>
> - d.
>
> _____
> Wikimedia-l mailing list
> Wikimedia-l@lists.wikimedia.org
> Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
> <mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

_____
Wikimedia-l mailing list
Wikimedia-l@lists.wikimedia.org
Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Re: [Wikimedia-l] NSA [In reply to]

peter.southwood at telkomsa

Jul 31, 2013, 11:14 PM

Post #36 of 45 (2047 views)

Permalink

And "non-western" countries probably go further if their technological capacity allows it. If you are not being spied on by "somebody" it is because no-one could be bothered or they havent got around to it yet, not
because any law protects your privacy.
P
----- Original Message -----
From: "Nathan" <nawrich@gmail.com>
To: "Wikimedia Mailing List" <wikimedia-l@lists.wikimedia.org>

> On Wed, Jul 31, 2013 at 5:53 PM, Matthew Walker
<mwalker@wikimedia.org>
> wrote:
>>>
>>> What surprises me is that anyone is surprised by any of this
>>> information.
>>
>>
>> It's one thing to have suspicions and theories about it; but if the third
>> party is constantly denying the allegations and with no recourse
there's
>> no
>> point in getting angry. Now that we have reasonable doubt, I hesitate
to
>> call it proof, we can start making tremendous amounts of noise.
>>
>> ~Matt Walker
>
> I think that's just naive. Of course it was always denied until it
> became impossible to deny it. That's how these things work. But I
have
> honestly assumed for many years that virtually everything transmitted
> over almost any electronic medium was collected and analyzed in
some
> way. That appears to be the case, and in fact, I expected them to
have
> gone further than they have. It seems that most of the data they
> collect is wiped within 3 days; that the data itself can only be
> analyzed under a fairly specific set of minimization rules after the
> approval of a senior executive in the administration, that the rules
> are drawn from generally accepted 4th amendment jurisprudence, etc.
>
> The cynic in me is also convinced that virtually all Western countries
> do the same sort of thing, if probably on a smaller scale. I would bet
> all the money I have that at a minimum the French, the English and
the
> Germans maintain roughly similar intelligence gathering programs.
But
> of course, they will deny it until it becomes impossible to deny it.
>
> _____

> Wikimedia-l mailing list
> Wikimedia-l@lists.wikimedia.org
> Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
> <mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Wikimedia-l mailing list
Wikimedia-l@lists.wikimedia.org
Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Re: [Wikimedia-l] NSA [In reply to]

peter.southwood at telkomsa

Jul 31, 2013, 11:28 PM
Post #37 of 45 (2045 views)
Permalink

Does the law actually require them to lie about data demands when questioned?
P
----- Original Message -----
From: "Nathan" <nawrich@gmail.com>
To: "Wikimedia Mailing List" <wikimedia-l@lists.wikimedia.org>
Sent: Thursday, August 01, 2013 1:52 AM
Subject: Re: [Wikimedia-l] NSA

> On Wed, Jul 31, 2013 at 7:11 PM, Michael Snow
<wikipedia@frontier.com>
> wrote:
>> On 7/31/2013 3:31 PM, Nathan wrote:
>>>
>>> And another thought - you know what unites most of the other
companies
>>> represented by the logos in that image? Leaks have confirmed that
most
>>> of them are the subject of secret orders to turn over huge amounts
of
>>> raw data to the government. They are all bound to secrecy by law,
so
>>> without permission none of them are permitted to describe or
disclose
>>> the nature or extent of the data demands the U.S. government has
made.
>>>
>>> Now if you imagine the puzzle globe on that slide implies that
>>> Wikipedia traffic is retained for intelligence analysis, it's a short

>>> hop to assume that the Wikimedia Foundation is also the subject of a
>>> blanket order transferring its server logs to the NSA.
>>
>> Facebook, Google, Yahoo, and Twitter, yes. But mail.ru? The shift from
>> "most" to "all" in the first paragraph may make it easy to assume the
>> similarity is universal, but it's ignoring the full context. That kind of
>> rhetorical shift is a favorite trick of conspiracy theorists, it's how
>> they
>> get you to make those short hops to unwarranted conclusions.
>>
>> --Michael Snow
>>
>>
>
> It's hardly a conspiracy theory. Given the differences between mail.ru
> and Wikipedia, I should think it would be clear why one might be
> subject to a direct demand for transferring data while the other is
> not. If anything, I think it's more reasonable to assume that
> Wikipedia (which shares many features with Google, Yahoo, Twitter,
> Facebook and other social networks) has been the subject of this kind
> of demand than that it hasn't. No one with direct knowledge would be
> able to do anything other than deny it, but we can easily see why data
> held by Wikipedia (including partially anonymized e-mails, file
> uploads, talk page communication, etc.) would be of interest to
> intelligence agencies.
>
> _____
> Wikimedia-l mailing list
> Wikimedia-l@lists.wikimedia.org
> Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
> <mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

_____
Wikimedia-l mailing list
Wikimedia-l@lists.wikimedia.org
Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Re: [Wikimedia-l] NSA [In reply to]

Thanks, This answers my question.
P

Post #38 of 45 (2047 views)
Permalink

----- Original Message -----
From: "Luis Villa" <lvilla@wikimedia.org>
To: "Wikimedia Mailing List" <wikimedia-l@lists.wikimedia.org>
Sent: Thursday, August 01, 2013 2:13 AM
Subject: Re: [Wikimedia-l] NSA

> On Wed, Jul 31, 2013 at 4:11 PM, Michael Snow
> <wikipedia@frontier.com>wrote:
>
>>
>>> Now if you imagine the puzzle globe on that slide implies that
>>> Wikipedia traffic is retained for intelligence analysis, it's a short
>>> hop to assume that the Wikimedia Foundation is also the subject of
a
>>> blanket order transferring its server logs to the NSA.
>>>
>> Facebook, Google, Yahoo, and Twitter, yes. But mail.ru? The shift
from
>> "most" to "all" in the first paragraph may make it easy to assume the
>> similarity is universal, but it's ignoring the full context. That kind of
>> rhetorical shift is a favorite trick of conspiracy theorists, it's how
>> they
>> get you to make those short hops to unwarranted conclusions.
>
>
> Thanks for the voice of reason, Michael.
>
> As a quick reminder here, before any conspiracy theories about
orders and
> data retention get out of control:
>
> 1) We've flat-out denied any sort of involvement in this, and we
continue
> to stand by that denial:
> https://blog.wikimedia.org/2013/06/14/prism-surveillance-wikimedia/
>
> 2) Take with a grain of salt, of course, but our understanding (based
on
> the few gag orders that have been made public) is that we could be
forced
> to not confirm having received a National Security Letter, but we can't
> actually be forced to lie about it. In other words, if we'd received one

> we
> would not be allowed to say "we've received one", but we also could not be
> forced to deny it - we'd always have the option to remain silent instead.
>
> 3) We understand that the rules cause some people not to trust our denial,
> and can't entirely blame them! That is why we've asked the government to
> change the rules, so that you can have more trust in us next time we issue
> the same denial:
> https://blog.wikimedia.org/2013/07/18/wikimedia-foundation-letter-transparency-nsa-prism/
>
> This is not to say that the http/https issue isn't important; like
> Engineering, we think progress on that issue is important. But it is
> important to keep "we don't yet deploy https as widely as we'd like"
> separate from "there are secret orders to transfer all our logs to the
> NSA."
>
> Thanks-
> Luis
>
> --
> Luis Villa
> Deputy General Counsel
> Wikimedia Foundation
> 415.839.6885 ext. 6810
>
> NOTICE: *This message may be confidential or legally privileged. If you
> have received it by accident, please delete it and let us know about the
> mistake. As an attorney for the Wikimedia Foundation, for legal/ethical
> reasons I cannot give legal advice to, or serve as a lawyer for, community
> members, volunteers, or staff members in their personal capacity.*
> _____
> Wikimedia-l mailing list
> Wikimedia-l@lists.wikimedia.org
> Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
> <mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Re: [Wikimedia-l] NSA [In reply to]

rupert.thurner at gmail

Jul 31, 2013, 11:57 PM
Post #39 of 45 (2057 views)
Permalink

On Thu, Aug 1, 2013 at 6:44 AM, Tim Starling
<tstarling@wikimedia.org> wrote:
> On 01/08/13 14:15, Anthony wrote:
>> On Wed, Jul 31, 2013 at 9:27 PM, Ryan Lane
<rlane@wikimedia.org> wrote:
>>
>>> I would be fired and jailed before I knowingly let that occur. If this
was
>>> the case I'd very surely not be working for Wikimedia Foundation.
>>>
>>
>> Key word there being "knowingly".
>
> I don't know why the NSA would sneak around in our data centres
> mirroring our ethernet ports if they already have almost all of our
> access logs by capturing unencrypted traffic as it passes through
> XKeyscore nodes.
>
> I think you should save the conspiracy theories until after we switch
> anons to HTTPS, that's when they will have an incentive.

tim, and ryan, that is not 100% true. since at least 2010 we know from articles like these:
* http://www.wired.com/threatlevel/2010/03/packet-forensics/
* https://www.eff.org/deeplinks/2010/03/researchers-reveal-likelihood-governments-fake-ssl
that man-in-the middle attacks are possible with and without HTTPS at XKeyscore nodes. the basic problem is, that wikipedia contents is stored in the U.S., and the site is using certificates issued in the U.S. the same country and legislation the NSA is located. this means the certificates can be compromised and users would not (easily) notice it.

the best sign against snooping internet traffic would be if wikipedia will change the hosting to a different country, and use a different

countries ssl certificate. you can bet, that the perceived impact on the U.S. business will be so huge that this intolerable practice will stop, at source, at NSA.

btw, ryan, you talked about firing and jailing - if you did not know that or if you knew it and ignored it, you should be fired or not work at WMF ;) it is _you_ who need to warn about the location beeing vulnerable, and it is _you_ who decide to use vulnerable digicert certificates. but you of course will not be jailed - this seems to happen to people revealing that xkeyscore exists ...

rupert.

Re: [Wikimedia-l] NSA [In reply to]

rarohde at gmail

Aug 1, 2013, 2:31 AM
Post #40 of 45 (2043 views)
Permalink

On Wed, Jul 31, 2013 at 5:13 PM, Luis Villa <lvilla@wikimedia.org> wrote:
> As a quick reminder here, before any conspiracy theories about orders and
> data retention get out of control:
>
> 1) We've flat-out denied any sort of involvement in this, and we continue
> to stand by that denial:
> https://blog.wikimedia.org/2013/06/14/prism-surveillance-wikimedia/
>
> 2) Take with a grain of salt, of course, but our understanding (based on
> the few gag orders that have been made public) is that we could be forced
> to not confirm having received a National Security Letter, but we can't
> actually be forced to lie about it. In other words, if we'd received one we
> would not be allowed to say "we've received one", but we also could not be
> forced to deny it - we'd always have the option to remain silent instead.
<snip>

If we are going to chase crazy down the rabbit hole, then it may be worth noticing that the NSL gag order makes it a crime to discuss NSL demands with anyone except A) personal legal counsel, and B) persons who are directly necessary to fulfill the demand. In particular, if I (as an individual) am served with an NSL then there is no provision allowing me to tell my boss or my subordinates unless I directly need their help to satisfy the request. If someone with root access were directly served with an NSL, it isn't obvious that WMF executives would ever learn about it. This is one of the ways that NSL gag orders are ridiculous.

-Robert Rohde

Wikimedia-l mailing list
Wikimedia-l@lists.wikimedia.org
Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Re: [Wikimedia-l] NSA [In reply to]

george.herbert at gmail

Aug 1, 2013, 2:56 AM
Post #41 of 45 (2056 views)
Permalink

The letters must be sent to the organization rather than an individual. The idea of going to an individual employee and strongarming them may happen, but the law around NSLs is specific.

The court cases to date indicate that if an individual employee got a US NSL and sued over it, the judge would likely take actions that would end the FBI agents careers.

Such individual strongarming would almost certainly use threats or MICE (money, ideology, compromise, ego) enticements and no paper trail to have to testify over in court later.

George William Herbert
Sent from my iPhone

On Aug 1, 2013, at 2:31 AM, Robert Rohde <rarohde@gmail.com> wrote:

> On Wed, Jul 31, 2013 at 5:13 PM, Luis Villa <lvilla@wikimedia.org> wrote:
>> As a quick reminder here, before any conspiracy theories about orders and
>> data retention get out of control:

>>
>> 1) We've flat-out denied any sort of involvement in this, and we continue
>> to stand by that denial:
>> https://blog.wikimedia.org/2013/06/14/prism-surveillance-wikimedia/
>>
>> 2) Take with a grain of salt, of course, but our understanding (based on
>> the few gag orders that have been made public) is that we could be forced
>> to not confirm having received a National Security Letter, but we can't
>> actually be forced to lie about it. In other words, if we'd received one we
>> would not be allowed to say "we've received one", but we also could not be
>> forced to deny it - we'd always have the option to remain silent instead.
> <snip>
>
> If we are going to chase crazy down the rabbit hole, then it may be
> worth noticing that the NSL gag order makes it a crime to discuss NSL
> demands with anyone except A) personal legal counsel, and B) persons
> who are directly necessary to fulfill the demand. In particular, if I
> (as an individual) am served with an NSL then there is no provision
> allowing me to tell my boss or my subordinates unless I directly need
> their help to satisfy the request. If someone with root access were
> directly served with an NSL, it isn't obvious that WMF executives
> would ever learn about it. This is one of the ways that NSL gag
> orders are ridiculous.
>
> -Robert Rohde
>
> _____
> Wikimedia-l mailing list
> Wikimedia-l@lists.wikimedia.org
> Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

_____
Wikimedia-l mailing list
Wikimedia-l@lists.wikimedia.org
Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Re: [Wikimedia-l] NSA [In reply to]

Mailing List Archive

Home > Wikimedia > Foundation > Page 2 1 2 View All

emijrp at gmail

Aug 1, 2013, 3:02 AM
Post #42 of 45 (2049 views)
Permalink

It is funny (but also sad) to see how people thought that Internet privacy was respected in Western world. Almost 99% only worried about China/Iran
Internet monitoring and censorship but we had here the most comprehensive
spy system logging every site you read.

Wake up!

Wikimedia-l mailing list
Wikimedia-l@lists.wikimedia.org
Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Re: [Wikimedia-l] NSA [In reply to]

wikimail at inbox

Aug 1, 2013, 4:39 AM
Post #43 of 45 (2041 views)
Permalink

On Thu, Aug 1, 2013 at 12:44 AM, Tim Starling
<tstarling@wikimedia.org>wrote:

> On 01/08/13 14:15, Anthony wrote:
> > On Wed, Jul 31, 2013 at 9:27 PM, Ryan Lane
<rlane@wikimedia.org> wrote:
> >
> >> I would be fired and jailed before I knowingly let that occur. If this
> was
> >> the case I'd very surely not be working for Wikimedia Foundation.
> >>
> >
> > Key word there being "knowingly".
>
> I don't know why the NSA would sneak around in our data centres
> mirroring our ethernet ports if they already have almost all of our
> access logs by capturing unencrypted traffic as it passes through
> XKeyscore nodes.
>

Especially not when they can get someone else to do it for them.

I think you should save the conspiracy theories until after we switch
> anons to HTTPS, that's when they will have an incentive.
>

And I thought Ryan Lane was talking about the future, not the past. I certainly was.

Re: [Wikimedia-l] NSA [In reply to]

rlane at wikimedia

Aug 1, 2013, 10:20 AM
Post #44 of 45 (2044 views)
Permalink

On Thursday, August 1, 2013, Anthony wrote:

> On Thu, Aug 1, 2013 at 12:44 AM, Tim Starling
<tstarling@wikimedia.org<javascript:;>
> >wrote:
>
> > On 01/08/13 14:15, Anthony wrote:
> > > On Wed, Jul 31, 2013 at 9:27 PM, Ryan Lane
<rlane@wikimedia.org<javascript:;>>
> wrote:
> > >
> > >> I would be fired and jailed before I knowingly let that occur. If this
> > was
> > >> the case I'd very surely not be working for Wikimedia
Foundation.
> > >>
> > >
> > > Key word there being "knowingly".
> >
> > I don't know why the NSA would sneak around in our data centres
> > mirroring our ethernet ports if they already have almost all of our
> > access logs by capturing unencrypted traffic as it passes through
> > XKeyscore nodes.
> >
>
> Especially not when they can get someone else to do it for them.
>
> I think you should save the conspiracy theories until after we switch
> > anons to HTTPS, that's when they will have an incentive.
> >
>
> And I thought Ryan Lane was talking about the future, not the past. I
> certainly was.

I'm talking about both.

- Ryan

Re: [Wikimedia-l] NSA [In reply to]

z at mzmcbride

Aug 12, 2013, 6:05 PM
Post #45 of 45 (1975 views)
Permalink

Anthony wrote:
>And I thought Ryan Lane was talking about the future, not the past. I >certainly was.

I think we should focus on the present, personally.

If a user goes to <https://wikipedia.org>, they're quietly redirected to <http://www.wikipedia.org>. This is true of a large number of domains (e.g., <https://wikimedia.org> and <https://mediawiki.org>).

This has been known about since at least October 2011 (cf. <https://bugzilla.wikimedia.org/31369>) and everyone seems to agree that
it's a pretty evil bug (a user knowingly tries to access a site over HTTPS and is unknowingly routed to HTTP). And yet it's August 2013 and the best
response we seem to have come up with is "install a client-side browser plugin" and "we're working on it."

It's difficult to believe that the Wikimedia Foundation is committed to user privacy when bugs like this go unresolved after so many months. This
bug will celebrate its second birthday in less than two months.

MZMcBride

Wikimedia-l mailing list
Wikimedia-l@lists.wikimedia.org
Unsubscribe: https://lists.wikimedia.org/mailman/listinfo/wikimedia-l,
<mailto:wikimedia-l-request@lists.wikimedia.org?subject=unsubscribe>

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 9

Talk:Access to nonpublic information policy/Archives/2013

< Talk:Access to nonpublic information policy

Please do not post any new comments on this page. *This is a discussion archive first created on December 9th 2013, although the comments contained were likely posted before and after this date. See current discussion or the archives index.*

Internal policy on ID collection

This was posted by Geoff on the Privacy Policy talk page but I think would be interesting to those here as well.

> **Wikimedia Foundation - Internal Policy**
>
> **Purpose**
>
> The Wikimedia Foundation ("WMF") may sometimes need to collect copies of identification documents ("IDs") from community members pursuant to established policies of WMF or the community. Examples where community members may need to identify themselves include the following:

Contents

- Candidates

Requirements sub-point A
Requirements sub-point B
Requirements sub-point C
Requirements sub-point D part I
Requirements sub-point D part II
Submitting new materials
Submission methods
Submission timeline
Use and disclosure intro paragraph
Use and disclosure sub-point A
Use and disclosure sub-point B
Penultimate paragraph
Final paragraph

Notifications

feedback from otrs agent

disagree with preservation of digital version of id papers
disagree with disclosure of agent private information to community members not bound to the non public information policy
ask for mandatorily notification of non public information disclosure about agent from WMF to concerned agent
Comments

Illegal

Statement from user:aschmidt

Stuff to think about

WMF board, FDC, etc.

Pedantic lawyerly point about use of "age of majority"

Community Committees

(http://meta.wikimedia.org/wiki/Board_elections/2011/en#Prerequisites_to_candidacy) for the WMF Board of Trustees

- Candidates (http://meta.wikimedia.org/wiki/Funds_Dissemination_Committee/Framework_for_the_Creation_and_Initial_Operation_of_the_FDC#Membership) for the Funds Dissemination Committee
- Recipients of WMF grants
- Representatives and agents of user groups and thematic organizations
- Community members (http://wikimediafoundation.org/wiki/Access_to_nonpublic_data_policy) with access to nonpublic user data information [GRB Note: we are currently not keeping such IDs on file.]

This internal policy summarizes the approach to be taken by WMF employees and contractors when handling and storing such community member IDs. The required ID depends on the criteria of the particular policy or practice, but may include copies of passports, driver's licenses, and other government-issued documents showing real name and age.

Collection, Storage, and Access

Copies of IDs provided to WMF by community members will be kept confidential, consistent with any applicable requirements of the WMF privacy policy (http://wikimediafoundation.org/wiki/Privacy_policy). Physical copies of IDs will be kept in locked cabinets designated for this purpose. Electronic copies of IDs will be protected by passwords or other electronic protections in files designated for this purpose.

Access to IDs will be limited to a "need to know" protocol determined by the program administrator. Usually that means only the principal administrators of a program will have access to those IDs. WMF will not share the IDs with outside third parties, unless required by law, covered by a non-disclosure agreement approved by Legal, or necessary to protect the rights, property, or safety of WMF and its employees and contractors.

Destruction

IDs will be kept as long as necessary to satisfy the need of the applicable policy and practice requiring the IDs. Such IDs will be destroyed as soon as the need for the ID has expired. Depending on the program, some IDs may need to be retained for a period of time for legal and financial purposes beyond the immediate purpose of the policy and practice. For example, IDs may need to be retained after the life of a grant to prove expenditure responsibility to government officials in the case of an audit. Check with Legal and Finance for any legal or finance record retention requirements.

V.1.1 (2013-03-14)

Illustrations

The following discussion is closed.

There are obviously a lot of things to talk about and if you aren't interested in this piece of it please feel free to start a new section with your discussion point/question/concern/etc. As you can probably see both here and on some of the other policies and draft pages we rolled out we're trying the idea of having illustrations and light humor in the text. These are not in anyway 'set' and may not appear in the final version if they're not appreciated. Legal documents tend to be lengthy, weighty and difficult to read (and rarely read at that) especially when you consider how many sites the average user visits. We want to make these documents as accessible as possible to as many people as possible. We hope to keep everyone's attention with the illustrations and a bit of levity. This is especially the case in the privacy policy but we've seeded them in a couple other locations as well. Do you like them? Hate them? Any specific ones work well or not work well? Should we think about another scene for a specific area? Jalexander (talk) 23:07, 3 September 2013 (UTC)

> I think the icons in the Privacy Policy are fantastic. Clear, and highly useful for navigating sections. The illustrations in both are fun, and I generally like them, but they're less useful for communicating the subject of the section. The top of the document says Rory is there to help explain the policy, but it doesn't feel like he's a narrator, more like an adornment. I think he should either be more tightly-integrated (perhaps with full SVG and color) or done away with in the name of simplicity. Steven Walling (WMF) • talk 05:18, 4 September 2013 (UTC)
>
> > I know color etc is an option for the final, it was just sketches now as the intro. Are you thinking more 'narration' ? Jalexander (talk) 05:20, 4 September 2013 (UTC)
> >
> > > Yeah I think if there's going to be a character, narration is probably more useful. Having to describe each section by putting it in a caption for the character to say is probably a good exercise in distilling the policies. Steven Walling (WMF) • talk 05:31, 4 September 2013 (UTC)
> >
> > The sketches of Rory are actually also meant to be up for community feedback -- the sketches are meant to be a start (that's actually why he is not in color and is unfinished). Final drafts of Rory will only be completed once community input has been obtained. We'd love to hear how he could be better utilized. Do you (the community at large) like the proposed sketches? Do you have ideas as to what else he should be doing to illustrate the concepts in the policy? What kind of narrative can we give him to bring the policy to life? How he could be better integrated? Privacy policies are notorious for being unreadable and hard to relate to. We hope that, with the community's assistance, Rory will be able to help with that. Mpaulson (WMF) (talk) 07:07, 4 September 2013 (UTC)

- **Note:** Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 20:44, 3 December 2013 (UTC)

Who's we?

The following discussion is closed.

"We will be accepting community comment until 15 January 2014. We look forward to comments on any aspect of the draft." ← Who's we? --MZMcBride (talk) 04:56, 4 September 2013 (UTC)

> Hi MZMcBride! "We" refers to the Wikimedia Foundation. This draft was the result of a collaborative effort between different departments, and coordinated by LCA. But the draft is not and cannot be complete without community input. We hope to hear from you during the community consultation period between now until 15 January 2014. During and following the community consultation period, we will be editing the draft presented today to reflect community suggestions and concerns, as appropriate, and then present the final draft to the Board for discussion and approval. Mpaulson (WMF) (talk) 05:15, 4 September 2013 (UTC)

A general aside: thank you so much for organizing these thorough public discussions and taking all of the feedback into consideration. I am learning a lot from this; and other community processes could as well. Including most of our global RfCs. –SJ talk 21:55, 24 October 2013 (UTC)

> Thanks Sj! The documents we introduce to the community are only a starting point. We learn so much from the community's participation and feedback during this process, and any resulting policies are better for it. =) Mpaulson (WMF) (talk) 22:15, 24 October 2013 (UTC)

- **Note:** Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 20:45, 3 December 2013 (UTC)

Wikipedia Day 2014

The following discussion is closed.

"We will be accepting community comment until 15 January 2014." ← What happens after January 15? Is there a public timeline anywhere? I assume at some point the Board has to approve the policy. --MZMcBride (talk) 04:57, 4 September 2013 (UTC)

> Hi MZMcBride! This draft is just that, a draft. We are working towards completing a final draft that has gone through vigorous interdepartmental and community feedback and will present that eventual draft to the Board for their review and discussion. The draft presented today will be reviewed and revised throughout the community consultation period in light of community feedback. After 15 January 2014, the draft will undergo any final revisions based on community feedback that

are still needed and then will be presented to the Board for discussion and potential adoption. Hope that helps! Mpaulson (WMF) (talk) 05:31, 4 September 2013 (UTC)

- **Note:** Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 20:45, 3 December 2013 (UTC)

Protect your access

The following discussion is closed.

Should contain something alla: 'users with these responsibilities will do the utmost to protect their accounts against unauthorized access, report immediately when they are aware such access has been compromised and follow the current agreed upon standards of usage of the account', the latter indicating that a user should use https if so defined in the current rules for checkuser access for instance. So i want to express that users can be assured that these people have a certain set of rules that they need to follow in order to be checkuser for instance, other than the 3 requirements of 18, ID'ed and pledged to confidentiality. TheDJ (talk) 07:01, 4 September 2013 (UTC)

Hi TheDJ! Thank you for your suggestion. Some of your concerns are actually addressed in the Confidentiality agreement for nonpublic information already.

As to your first suggestion, users with these responsibilities must "Comply with the Privacy Policy; the Access to Nonpublic Information Policy; and any other applicable and nonconflicting community policy relating to nonpublic information" and "Refrain from disclosing nonpublic information to anybody, except as permitted under those policies". Do you think adding another requirement that they must generally strive to protect their accounts against unauthorized access in addition to the requirements I mentioned above would be beneficial?

As to your second suggestion, they also have the duty to report disclosures under the terms of the confidentiality agreement -- they must "Notify check-disclosure at wikimedia.org and provide an explanation within 10 days if [they] disclose nonpublic information to outside parties, such as law enforcement" and "in case of a violation of this agreement, including improper access, use, or disclosure of nonpublic information...[they] will notify the Wikimedia Foundation about the violation immediately".

And finally, regarding your third suggestion, there are currently discussions within the Foundation as to how we can provide more secure connections to users with access to nonpublic information, but a perfect solution has not yet been found. https is certainly an option, but not one that we can apply everywhere. For example, https can actually hinder a user's ability to access in certain countries, like China. Your suggestion is a good one and one that we would like to implement in the future once we have methods of providing more secure access to users with these responsibilities (and hopefully all users eventually). Mpaulson (WMF) (talk) 18:13, 11 September 2013 (UTC)

In hindsight, I don't care as much about those 3 specific things, they could be internally documented. I want to make it clear to readers that the people who have this access to private material are required to act following the operational guidelines that are set for their specific 'position'. If you have "Minimum requirements for community members applying for access to nonpublic information rights", then (a) is a eligibility requirement for the functionary, (b) is an identification requirement on the functionary, (c) is an ethical agreement that the functionary signs with the foundation (which represents the community), (d) is a requirement onto the foundation about the proof talked about in a, b and c. My statement would have to express the 'burden' that is placed onto the functionary when he operates in his function to operate with the methodology that is expected of the function/office. (this could then include requirements on using https all the time for instance, protecting your password in general etc, but also for instance keeping non-public logs of actions for instance). We have trusted these users with some access and we require them to be careful with that access. When the library lends you a book, you don't bring it back all torn up. I don't know, it's complicated :D TheDJ (talk) 13:19, 23 September 2013 (UTC)

That's a fair point. What about if we change the last bullet point under (c) to "when and to whom they may disclose the nonpublic information and how they must otherwise refrain from disclosing nonpublic information to anybody, except as permitted under applicable policies" and add an additional bullets point saying "how they must safeguard their accounts from unauthorized access" and "when they must report disclosure of nonpublic information to third parties or improper access, use, or disclosure of nonpublic information"? We could would also add an additional bullet point in the confidentiality agreement under the "Protection of nonpublic information" section stating "Reasonably safeguard your account from unauthorized use." Let me know what you think of the additional language. Mpaulson (WMF) (talk) 23:47, 15 October 2013 (UTC)

- **Note:** Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 20:51, 3 December 2013 (UTC)

Why should copies of the photos ID be retained ?

The following discussion is closed.

While I can understand that the WMF would in some cases need to have confirmation of the identify of a volunteer, it is not clear to me why it should keep a copy of the actual photo ID. Whenever I need to be authenticated, I show my ID, someone checks that the information they have recorded is correct, then ticks a box on a paper form saying "ID checked" and confirms by signing it -- without keeping a copy of the ID. Usually, only banks require an actual copy of the ID. Why wouldn't it work ? In Switzerland, sending a copy of a photo ID is enough to authentify oneself in order to get access to most documents (medical record, bank accounts, criminal record). However, simply knowing the information printed on the ID does not open any such door. Could we setup the system in this way ? I know that the probability of someone misusing the data stored at WMF is small, but the potential consequences in case of problems are **huge**.

Another scheme that was suggested a while ago is that chapters (in countries where they exist), or a lawyer mandated by the chapters, should/could be used as a trusted 3rd party that would authentify such photo ID and send the relevant information to the WMF. This would have the added advantage that, for quite a few volunteers, they would not have to send any document to a foreign country (they may not even have to make a copy of the photo ID). Additionally, local people know what official photo IDs look like, and they could see the original document, reducing drastically any possibility of fraud. To me, this sounds like an appealing scheme, no ?

Finally, I am wondering about the following sentence:

> *The Wikimedia Foundation will not share submitted materials with third parties, unless such disclosure is (A) permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department*

I read that as "the WMF will not share submitted materials with third parties, except when it has itself approved to do so". That seems like a very weak protection. Shouldn't there be a explicit limitations of the cases in which such a transfer of material can happen ?

Thanks in advance ! Schutz (talk) 09:24, 4 September 2013 (UTC)

> FWIW, that's *not* an appealing scheme to WMIT, as clearly stated by our president and board. Of course if the WMF hired EU firms to handle such stuff many would be happier. --Nemo 21:04, 4 September 2013 (UTC)
>
> > Which problems do you see with this scheme ? Legal, practical, others ? Schutz (talk) 09:14, 5 September 2013 (UTC)
> >
> > > WMIT doesn't want and can't be an *agent* of WMF for anything. --Nemo 12:30, 5 September 2013 (UTC)
>
> Hi Schutz! One of the main reasons we are requiring identification from community members with this level of access is accountability. The information that is entrusted to these community members is very sensitive and knowing who has access to that information is a big part of working towards accountability. In the examples you stated where identification is required to get access to other information, you presumably get checked every time you try to access that secured information. Here, in situations covered by this policy draft, where the access is continuous, retaining a copy of the id submitted seems more logical that attempting to check someone's id every time they attempt to exercise their access rights.
>
> As to your second comment about whether it should be WMF that holds the ID, Nemo is correct in that chapters should not be seen as agents of WMF. That also doesn't help the community members who do not have chapters in their countries (or if in their countries of residence, chapters that are geographically close to where they reside). Appointing third-party attorneys or bodies to collect and hold the ids locally is administratively and legally challenging as well. Do we appoint an attorney in every location where there is a community member who submits an id? If the attorney is appointed, who is the attorney's client -- the community member or WMF? How would be ensure that all of these attorneys retain a copy of the ID properly (both in length of time and with proper security measures in place)? What happens if an attorney leaves practice and doesn't tell us or the community member? We believe that whatever risk associated with WMF's storage of the ids is considerable less than if the ids were stored by third parties.
>
> And finally, as to your third comment, I think some clarification about what kind of situations the sharing of these materials section is meant to cover will help guide this discussion. First, though, I'd like to note that there are limitations on when we can share the materials with third parties, specifically: "(B) required by law; (C) needed to protect against immediate threat to life or limb; or (D) needed to protect the rights, property, or safety of the Wikimedia Foundation, its employees, or contractors." Do you believe these situations are reasonable?
>
> I do understand your concern with regard to "(A) permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department" though. The reason why we included this was to address situations where a person helping with security of the materials is a contract employee who has signed a non-disclosure agreement with the Foundation or if we hire a company (who has signed a non-disclosure agreement) to help secure materials submitted electronically and they have to handle the materials in the course of helping us. The point of the Foundation's non-disclosure agreements with these sorts of parties would be to secure similar or greater protections than those promised in this policy. Does that make sense? If so, do you think the language of (A) could be changed to make this clearer?
>
> Hope this helps and look forward to hearing more of your thoughts on these topics. Mpaulson (WMF) (talk) 20:13, 11 September 2013 (UTC)
>
> > Sections (A) and (D) jumped out at me as well. They both appear to offer quite fragile protection for those submitting "non-public information" to the WMF - which is, you might agree, ironic. I think A should be tightened up to narrow the circumstances in which information is shared (such as including provisos that it will not be for commercial use, and that no outside entities will retain a permanent copy of any personally identifying information). I think D also has holes

big enough to drive a truck through, because "rights and property" of the WMF, its employees and contractors is a pretty broad category. Does that mean if permanently deleting the data from the hard drive of a contractor might damage that contractors property, the policy allows them to retain the information? I understand that the natural inclination of attorneys representing a client is to draft as broadly as possible in favor of the client, but that is the wrong impulse when considering the responsibility of the WMF to protect the identifying information of both readers *and* volunteers. Since the volunteers are potentially sharing much more sensitive information, a little more weight on protecting them needs to be added to this policy. Nathan T 19:25, 14 October 2013 (UTC)

> Hi Nathan! Thank you for sharing your thoughts. As to (A), what do you think about tightening the language to something like this: (A) permitted by a non-disclosure agreement that (1) has been approved by the Wikimedia Foundation's legal department; (2) allows for only non-commercial use of the submitted materials; (3) allows for use by the recipient of the submitted materials in accordance with the Wikimedia Foundation's instructions; and (4) obligates the recipient of the submitted materials to return or destroy all copies of the submitted materials in its possession within a reasonable time following the recipient's need for the information.
>
> And as to (D), I understand why you think the provision is broad. It is meant to be, but not because we are trying to draft broadly in favor of WMF as our client. We wrote it broadly because it was meant to cover unlikely and, to a certain extent, impossible-to-predict scenarios that can be hard to enumerate. I admit, I'm a little confused by your example of how this provision could be used. If permanently deleting the data from the hard drive of a contractor would damage that contractor's property, that doesn't mean that the policy allows them to retain the information. Clause (A) would cover how we were permitted to give access to the information to the contractor, but not how long they could retain the information. Clause (D) covers completely different scenarios where we would be permitted to share information. For example, in the unlikely scenario where our building was broken into and our equipment was stolen or where our computer systems had been compromised and we had a good reason to believe that it was someone whose personal information we had, we would be permitted under this clause to report that person to the appropriate authorities. Again, it's hard to imagine every possible scenario where this clause may be helpful. I frankly hope we never, ever have to use the clause. We do not take the disclosure of personal information lightly. In fact, we are loathed to disclose information short of being legally compelled to do so or for safety reasons. That said, we're very much open to editing (D) in a way that would better illustrate what that clause is trying to cover and I'd love to hear any suggestions you may have. What about something like this: (D) needed to protect the safety of others or WMF staff, contractors, systems or property?
>
> I look forward to hearing your thoughts on my suggested revisions as well as any suggested revisions you may have. Mpaulson (WMF) (talk) 19:54, 16 October 2013 (UTC)
>
> > You still have not answered the question of why the ID has to be retained over retaining the Data in it. And I for one will never, ever accept the property clause of this proposal. That is simply unacceptable. **Snowolf** How can I help? 20:07, 17 October 2013 (UTC)
> >
> > > I second Snowolf's sentiment; I don't think our data should be used for non-commercial purposes, either. I also suggest to obligate any recipient of our sensitive personal information to return or destroy all copies *immediately* following their need for it. On a related note, why would you share this sort of personal information with anyone at all? I don't really see any need for any contractor or WMF staff member except perhaps two or three people (take Philippe and Geoff from Snowolf's example above) to have access to it. odder (talk) 21:08, 17 October 2013 (UTC)
> > >
> > > > Outside counsel is the only thing I can think of. **Snowolf** How can I help? 21:28, 17 October 2013 (UTC)
> >
> > "You still have not answered the question of why the ID has to be retained over retaining the Data in it." I think we'd probably be OK with simply retaining the data. We'll have to think about it some more, but the ID portion of the proposal was mostly based on past practice. Would keeping data, rather than the ID, resolve your other concerns about us collecting this data? -LVilla (WMF) (talk) 22:43, 25 October 2013 (UTC)
>
> On the question of "property" as a "loophole": the idea here is really primarily about our technical infrastructure; e.g., if a volunteer developer who we have ID'd starts attacking the site, we'd like to be able to use this information to help identify them and protect the site. So does it feel more narrowly tailored if we replace "property" with "infrastructure"? -LVilla (WMF) (talk) 19:57, 1 November 2013 (UTC)

- **Note:** Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 20:51, 3 December 2013 (UTC)

CheckUser policy

The following discussion is closed.

As already addressed here, let me reiterate my remark (that still remains) about the revelation of **the link** between an IP and an account, as it is a

compound of private and public data.

Aside from this point, I am happy with the changes and the new layout of the page. Elfix 08:00, 5 September 2013 (UTC)

> Hi Elfix! Just to be clear, are you referring to the the link between logged-in accounts and anonymous accounts in situations like sock-puppet investigations? If so, I think the Privacy Policy draft most directly addresses this situation in the To Protect You, Ourselves, and Others section...specifically: "We may need to share your personal information if we reasonably believe it is necessary to enforce or investigate potential violations of our Terms of Use, this Privacy Policy, or any Foundation or user community-based policies." To a certain extent, public inference of the links between particular IPs and accounts are unavoidable in sock-puppet investigations and are permissible due to the sentence above. I do understand your concern that it is not as clearly stated with in the Access to nonpublic information policy draft or the Confidentiality agreement for nonpublic information as to whether the community members handling these investigations are permitted to disclose this information in the course of their investigation. I'd love to have this stated more clearly. Do you have any suggestions as to how we could make it clearer in either the Access to Nonpublic Information Policy draft or the Confidentiality Agreement draft? Mpaulson (WMF) (talk) 19:28, 11 September 2013 (UTC)
>
> > Thank you for your response. I didn't pay enough attention to the bit you are quoting, and it is, I think, clear enough. Thanks! Elfix 21:33, 12 September 2013 (UTC) However, in "We may need to share your personal information", the use of the "share" verb may not be clear here (share with whom?). Elfix 18:50, 13 September 2013 (UTC)
> >
> > > Yes, the language in the Privacy Policy draft is relatively broad because it's trying to cover any possible person/entity that may have to be alerted depending on the type and severity of the alleged violation committed by literally anyone who can access the Wikimedia Sites. I'm not sure if there's a way for us to do an exhaustive list to cover every possible scenario. We do try to be more specific in the Access policy draft about to whom and under what situations community members with access rights may disclose information to though. Mpaulson (WMF) (talk) 00:36, 16 October 2013 (UTC)

I have a follow-up hypothetical question for you. The case of the UK where random IPs in dynamic ranges typically don't do anything other than reveal you're in the UK is quite clear cut. However, let's say that a person's IP reveals private information about them (e.g. they're on 130.88.0.0/16, a range owned by the University of Manchester). In terms of the policy, does this change the above advice that it's permitted to disclose that IP to someone in the case that they, say, want to write an abuse complaint to the University of Manchester? --Deskana (talk) 09:25, 15 October 2013 (UTC)

> Hi Deskana! Thank you for your question. Do you mean whether it would be ok for a community member with access rights to disclose a nonpublic IP that is specific enough to identify that the IP falls within a range owned by the University of Manchester and is associated with a user account? It would be ok if the disclosure was made as part of an investigation of potential violations of a policy and the IP was disclosed in the an abuse complaint "to assist in the targeting of IP blocks or the formulation of a complaint to relevant Internet Service Providers" (that latter if UM was also the ISP). Otherwise, no, they should not disclose the IP. Did I understand your hypo correctly? Mpaulson (WMF) (talk) 00:36, 16 October 2013 (UTC)
>
> > Perhaps a more specific and common situation: IP address provides some sort of information about the user (e.g., it's a business IP, and researching it through WHOIS will identify the business). There are a pile of socks, and there are no good users on the IP. Standard practice is to at least softblock the IP while also blocking the socks. However, it takes no imagination at all to make the association with the IP address and the socks just by looking at the CU's block log. So....is the CU violating policy by blocking both the socks and the IP? Risker (talk) 02:27, 16 October 2013 (UTC)
> >
> > > Hello @Risker:, this is a tough situation. For the same reason that Michelle explained above, it's allowed under the current version of the policy. However, upon a closer reading of the new draft privacy policy and access to nonpublic information policy, this is not addressed directly. To make it clearer, we could add to "Use and disclosure of nonpublic information", section (b):
> > >
> > > > *Disclosures of nonpublic information may be made to: ... the public, when it is a necessary and incidental consequence of blocking a sockpuppet or other abusive account; ...*
> > >
> > > This would make it acceptable under the privacy policy/access policy for CheckUsers to conduct the type of blocks that you suggest. Of course, projects could also set a higher bar in their local CheckUser Policy, if they don't think this is appropriate. This is a tough question, but the policy can be accommodating if its necessary for CheckUsers to do their job. Thanks, Stephen LaPorte (WMF) (talk) 21:13, 1 November 2013 (UTC)

- **Note:** Given how long this thread has been stale and the fact that it appears to be resolved I'm going to archive this in a couple days unless reopened. Jalexander--WMF 20:54, 3 December 2013 (UTC)

Data retention forced by what law?

The following discussion is closed.

Current draft says the collected ID will be retained for 3 years. I'd like to ask this measurement is forced by what law. In my country the data retention criteria are fixed in written law, and unless the data retention is required by law the data must be destroyed immediately the purpose of data collection is satisfied. Data retention without legal basis will be only the risk that the data would be compromised. There are several accidents that personal information of 35+ millions of people are leaked. If the data retention is based on US law, please let us know where the legal basis is, and if not, please don't retain the data. Best regards. – Kwj2772 (msg) 14:34, 25 September 2013 (UTC)

> The same here in Italy, data must be destroyed *as soon as possible* on request. --Vituzzu (talk) 18:30, 14 October 2013 (UTC)
>
> I doubt the specific time period is mandated by law, although there are various statutes of limitation - many of which in California are three years or less. I'm just speculating, but other circumstances that might dictate data retention times are contracts, grant terms, government funding, participation in certain state or federal programs, etc. Unlike European and other jurisdictions, the U.S. does not have a general limit or prohibition on retaining private data. And while many users live in jurisdictions where those rules apply, they do not govern the behavior of the WMF. Nathan T 19:37, 14 October 2013 (UTC)
>
> > But still I'm subjected to EU law. --Vituzzu (talk) 10:46, 15 October 2013 (UTC)
> >
> > > Hi Kwj2772, Vituzzu, and Nathan. Thank you for your questions. While there are data retention periods that are mandated under US law for specific situations (such as tax purposes, retention of client files, etc.), Nathan is correct in that there is no general law in the US that governs data retention periods and WMF is not subject to EU retention laws. Organizations are free (absent specific situations where particular laws apply) to set their own data retention periods for different types of data. Mpaulson (WMF) (talk) 17:49, 18 October 2013 (UTC)
> > >
> > > > Even if you're not subject to EU laws on data retention, it might be well worth looking into them and perhaps adopting some of the regulations; there are many stewards, checkusers, oversighters and OTRS members who are EU citizens, and I'm sure some of them would like you to adopt these higher standards even if you're not obliged to do so by U.S. law. odder (talk) 17:59, 18 October 2013 (UTC)
> > > >
> > > > > I would be interested in hearing from you guys about what you think would be an appropriate retention period? If you have thoughts on this issue, please leave them in the retention thread. (I'm trying to keep the responses on that topic in one place so they are easier to track.) Thanks! Mpaulson (WMF) (talk) 22:56, 25 October 2013 (UTC)

- **Note:** Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:02, 3 December 2013 (UTC)

Re-identification and retention of data vs. the NSA

The following discussion is closed.

I have identified to the Foundation a couple of years ago upon receiving access to OTRS, and my identification has been confirmed by a WMF staff member. Therefore, I cannot see anything that changed in those past few years that would require me to re-identify with the WMF, and send them a scan of my ID again.

I am also very concerned and feel deeply uneasy about (re-)sending a copy of my ID--which is probably one of the most delicate information the WMF can hold--to an organisation in a country where countless government agencies can force them to reveal any and all information they want, or even get the information without a court's approval or the subject's awareness. (Yes, I'm looking at the U.S., the recent scandals around the NSA, and the worryingly broad scope of the CIA and other intelligence-gathering organisations.)

If a re-identification or change of the current policy is required, I would prefer to be able to identify to an organisation, group or an individual acting in professional capacity in a jurisdiction which guarantees the best possible protection of my personal information (see data retention policy issue brought above by Kwj2772), and where I will have the ability to protect my personal liberty in the most effective way possible, without having to spend tens of thousands of dollars and fight against the ever-expanding appetite of government intelligence agencies. odder (talk) 16:12, 14 October 2013 (UTC)

> This policy will make most of most active users leave the Project, I wonder who will eventually checkuser, oversight, etc upon these basis.
>
> - These changes are made by a completely USA-centric perspective, without any care for other Countries' jurisdictions (for instance the three-years terms violates Italian law) but also different cultures (for instance in European countries law tends to avoid lawsuits and *subpoena is completely insane by our perspective*). You shouldn't forget users living outside USA are subjected to their respective countries' laws.
> - These changes make the policy even more blurry, on a theoretically basis everything can be meant to *prevent damages to WMF's properties*.
> - Also, a confidentiality pledge is not bad but still it doesn't take into any consideration the whole World outside USA, both the agreement and the way to sign it might have no value at all for people living outside USA.
> - This new version gives legal value to "normal" emails, I don't know if this might have any value in USA, but this is utterly ridiculous here in EU.
>
> Finally I have a simple question: each change is supposed to fix some practical problem, so, **which problems are supposed to be fixed by these changes?**
> --Vituzzu (talk) 17:35, 14 October 2013 (UTC)

> Hello @Vituzzu: Michelle has provided more detail on why these changes are being considered below, at Rethinking the access policy: Response to recent feedback. Does this answer your question? Stephen LaPorte (WMF) (talk) 21:39, 1 November 2013 (UTC)

- Anything could be argued to be a damage to WMF's properties. If I go out and criticize the WMF, I am damaging its properties in a way. I do not think that I would be able to continue serving in my capacities should such a flimsy policy be implemented. I was already uneasy about submitting identification when I did so some years back, and that was with the assurance that it would be destroyed after my identity was confirmed. My concerns are magnified by the idea of the documents being retained. I recall a lengthy thread on some OTRS mailing list in 2008 or 2009 about the processing of identification informations, where several volunteers were raising questions about the then current practices. Some of the points made then should be taken into account now, if the WMF wishes to go ahead with this. **Snowolf** How can I help? 18:08, 14 October 2013 (UTC)

> It's also funny to read *WMF employees and contractors...hey I'm a contractor making a research about the way different countries print IDs!* Seriously, nobody knows how the fuck is hard to sue one of these unfaithful contractors from the other side of Atlantic or Pacific Oceans? Also, though my main question still is "why is this change needed?" I have also another question: "why so few announcements have been made in comparison with the asphyxiating spam we are used to receive for every futile change in some useless MW's functionality?".
> --Vituzzu (talk) 18:28, 14 October 2013 (UTC)

> I'm more concerned about id theft and data leak than anything else. I don't like the idea of somebody storing a scan of my driver's license, which could easily be used for nefarious purposes by malicious individuals, on a networked server. Would the data be taken from the "secured" inbox, encrypted, and then placed into an air-gapped server? Reaper Eternal (talk) 18:40, 14 October 2013 (UTC)

> > That is my worry too. I also don't want the printed stuff to be in a some office locker. It should be in a serious safe. We should have a list of those with access, etc.. The issue of the air-gapped server was discussed at length in the otrs mailing list in a thread from I belive 2008 or 2009. I wish I could find it as the point made there are just as relevant now. **Snowolf** How can I help? 19:31, 14 October 2013 (UTC)

> > > The discussion you seem to have in mind took place in February 2011. You can see the relevant thread on Wikimedia-l (then Foundation-l) here (http://lists.wikimedia.org/pipermail/wikimedia-l/2011-February/110390.html); there was also a discussion on the OTRS wiki cafe (https://otrs-wiki.wikimedia.org/wiki/Caf%C3%A9/Archive_6#Identification_of_OTRS_agents). This post on Foundation-l (http://lists.wikimedia.org/pipermail/wikimedia-l/2011-February/110392.html) mentions threads on the private otrs-en-l and otrs-permissions-l mailing lists, but I am no longer subscribed to any of them, so I can't check the archives. I hope this will help with your search. odder (talk) 20:19, 14 October 2013 (UTC)

I can only agree with odder, Vituzzu, Snowolf and Reaper Eternal. This proposal is highly outrageous. Like Vito I can't see any problem which would be fixed by this. I plan to resign as a steward if it passes. Some complaints, in addition to those already mentioned above:

- At first it is stated (in "(d)(i)") that the data will not be shared by the WMF etc. bla bla except if *(A) permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department; (B) required by law; (C) needed to protect against immediate threat to life or limb; or (D) needed to protect the rights, property, or safety of the Wikimedia Foundation, its employees, or contractors*. As wide-ranging as that is formulated, it st)ll gives some "severe" criteria. Then in the next section ("(ii)") however we read *"the Wikimedia Foundation or a user community committee will need to contact a community member who formerly had access rights about his or her usage of those rights. For example, the Arbitration Committee may need to complete an ongoing case they are examining or the Wikimedia Foundation may need to notify you of receipt of a legal document involving that community member."*
  - That the Foundation may need to contact a user about how/why he used CU in a certain way or so certainly does not always mean that they may need to do it to protect the Foundation's glorious property. Nevertheless just before such a requirement was established. So why is such a fishy reason used for justifying keeping the data? Even more dubios the next reason:
  - What the heck is a "user community committee"? The next sentence of course suggests it is "the Arbitration Committee". What the heck is "the Arbitration Committee"? There is no global arbcom or anything. Just some projects happen to have one. This proposal was clearly written by someone focussed on enwiki.... but apart from that, it sounds like any community may just establish a committee that then uuuurgently has to ask some questions. How nonsensical. If at all, there need to be clear criteria for such an (arb?)com - which criteria it must fulfill (e.g. selection method, identification of members themselves?) in order to be considered to be allowed access to such data.
  - Additionally, how would such a "the Arbitration Committee" contact the user? (It also of course seems like we must assume someone who is not active anymore, as otherwise he could simply be asked on his talk page or by mail. Right to vanish?). Get the address and mail him? Will WMF visit or sue him on behalf of "the Arbitration Committee" until he answers?
  - "The Foundation may need to notify you of receipt of a legal document involving that community member". This sentence totally makes no sense. You == "that community member"? And what a legal document? A legal document calling for "that community member" to be arrested?
- The "destruction process" is also total bogus. A user who no longer has CU/OS access should notify stewards, who then inform the Foundation. First, stewards notice anyway when CU/OS removal happens, because they do it. Second, it reads like the data will only be destroyed if the user "notifies stewards" at all. Can a steward just tell the Foundation sua sponte that someone lost CU/OS or only when the user himself requested it? Third, why stewards at all? They are volunteers, they might also simply forget to impart the "wish for destruction" in a case, etc. If this outrageous proposal succeeds at all, there **needs** to be a qualified WMF staffer who watches Special:Log/rights for removal of CU/OS/steward and is also contactable by users who lose this access, just to be sure, and who sees to it then that the data is really destroyed after the prescribed time. And then not only "in a timely manner following the three (3) year period" but immediately! It is barefaced to say data is stored for maximum 3 years after the loss of access, and then only execute this "in a timely manner" i.e. when we want.

--MF-W 21:57, 14 October 2013 (UTC)

> I fully agree with the opinions expressed above me in this section, but I'd like to expand on the problem with giving power to a "user community committee" in this case. There are very, very few projects which have an ArbCom or similar body (and no such body exists at the global level), so these groups shouldn't be included in any policy as the norm. If they are ever mentioned, it should be as an after-note in a different sect)on explaining special cases.

> On this note, the role of a "user community committee" isn't defined at all here. Will they actually have access to scans of ID? It seems to imply that the Foundation is keeping them around so they can look at them later... to contact me or "complete an ongoing case". What does that mean? Can I go to lessthantencontributors.wikipedia.org, become an admin and arbitrator, and then get access to all identified people's documents? Why would an arbitration community, or a "user community committee" even need that sort of information when filling the definition of their role? Google defines arbitration as "The use of an arbitrator to settle a dispute", not "A body who looks at confidentially-submitted IDs and stalks former contributors". Some clarification here would be useful. Ajraddatz (Talk) 23:31, 14 October 2013 (UTC)

- As can be deduced from my contributions, I am a resident of the state of California, so there is no getting around California state law in my case. I can see where this proposal comes from, and I believe there are valid points here. But I believe in some areas that this proposal goes too far. There are several loopholes as mentioned by the others above. I still have yet to go through this in fine detail, but one thing that doesn't strike me too well is the clause saying, in effect, "if you leak private data, we will sue you." Of course, I believe that in some cases legal action may be appropriate, such as a steward/CU willfully violating people's privacy. But the way it's written, it implies that not even our most trusted functionaries are ... trusted, and that honest mistakes will be swiftly and soundly punished by consequences in real life. If that is to be the case, then we might as well have WMF take over all functionary positions, because I don't think there will be many takers for such a *volunteer* role. Functionaries are editors, and their privacy should be protected too. --**Rschen7754** 23:26, 14 October 2013 (UTC)
- I'm also fairly alarmed by this change, on two fronts. **First**, the general idea of the WMF keeping copies of documents of mine that could be used to do everything from open a bank account to getting a duplicate passport is alarming. In the cases of other organizations that have such documents from me, the organizations have track records and demonstrable processes for protecting the data, both physically and electronically (as well as there usually being established legal/governmental processes that hold the organizations to their promised non-disclosure and protection). The WMF, on the other hand, proposes to get these documents from us with a promise of, "We'll totally lock that filing cabinet and password-protect the file!" Unfortunately, organization at the WMF often seems to be lacking, and I simply find myself unable to muster enough confidence in its ability to make this one particular procedure bulletproof, this one time, the first time.

  Second, the idea that they won't disclose my personal information, except when they decide they can disclose it to whoever they want ("permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department") or when they decide it's in their best interest ("needed to protect the rights, property, or safety of the Wikimedia Foundation, its employees, or contractors"), amounts to "so, we won't give people your passport, except when we will, which might be pretty often, who knows?"

  I was and am perfectly fine with letting someone at the WMF check over my documents to verify my identity (as, indeed, they have already done). But before I'm comfortable with them keeping copies of it for their own purposes, I need to see far, far more detail about a) how my rights (not the WMF's) will be protected as far as who gets copies of my information, and b) how, exactly, my data will be protected. "We'll put a padlock on the cabinet" isn't adequate; I'm looking for something more like "We have designed storage procedure X and had it audited by independent security firm Y, which verifies that this procedure is state-of-the-art and resistant to both tampering and hacking to a level standard in the data-protection industry." The contents of people's passports, identity cards, or driver's licenses isn't the sort of thing you can protect using "agile" development where you start with something that sort of works and then iterate to improve when you find bugs. You need to have proven security from the very first moment, because if this goes wrong, it won't be annoying for the people whose identities are stolen, it will be *catastrophic*. Fluffernutter (talk) 00:29, 15 October 2013 (UTC)
- Man9`good points. On the other hand, WMF has to have some way of knowing who tools holders are (especially CU), and it should be a bit more than WMF staff memory. Perhaps a one-time ID check and registering a name somewhere (plus perhaps other data, such as date of birth, but not full ID scans) would address the concerns above? Pundit (talk) 05:15, 15 October 2013 (UTC)
- I **strongly oppose** this. I echo Snowolf's concerns and with the security breach at Labs, I do not feel comfortable with this change. Echoing what Vituzzu said, I would be one of these users who would leave. Elockid (talk) 22:33, 15 October 2013 (UTC)
- I am in agreement with my colleagues above. Furthermore, I understand why certain contracts mention the possibility of legal action, but these contracts then must include compensation for the signing party. Just like I refuse to sign publication waivers that make me solely responsible before the law if some madman decides to claim my images as his and sue, I feel uncomfortable with the present framework. People who have to answer before the law must know precisely when they are within their purview or not, they must enjoy legal support in case of problem, and they must be paid for the trouble. I am a volunteer here, and while I do pro bono work out of idealism, the pleasure I derive from the very act of contributing is also a factor; having second thoughs about prosecution in the USA for every action I take makes contribution less enjoyable, and there is a point where a contributor, without making a big fuss about it and without necessarily hitting a particular red line, will decide that the boat is overloaded and shrug off their commitment to the projects. Rama (talk) 06:35, 16 October 2013 (UTC)

Explain data retention in the policy itself

I think it would be very helpful for a complete and clear statement from the WMF, within the policy itself, on why identification is necessary and separately why it is necessary to retain hard copies of government-issued identification of volunteers. Many non-US countries have a very different culture when it comes to personal and private information, and are likely to have (and already are having, in some cases) a much stronger negative reaction to this than Americans might overall. It's unfortunate that the policy sort of glosses over the justification for data retention without making a really strong argument in favor of it, so perhaps Geoff and his team can remedy that? **Nathan** T 19:41, 14 October 2013 (UTC)

> Nathan, I know you've already seen this, but to anyone else following this thread, you may be interested in the discussion below regarding why we would like community members with access rights to identify. I'd also like to note that we are open to the possibility of retaining only identifying information about these community members rather than copies of identification documents themselves. We'd love to hear from other community members on this subject. Thanks in advance (and specific thanks to you, Nathan, for your patience as we respond to everyone's input.) Mpaulson (WMF) (talk) 23:18, 31 October 2013 (UTC)

Who needs to identify at all now?

>>Any community member who has been granted access rights and has not previously identified under the previous "Access to nonpublic data" policy (adopted 2007) has sixty (60) days to meet the Identification Requirements of Section 2(b) and the Confidentiality Requirements of Section 2(c) of this Policy."<< Do such users still exist? Afaik nowadays everyone who has access to CU/OS should be listed on IN. --MF-W 22:12, 14 October 2013 (UTC)

> If I remember correctly, there might still be some OTRS agents who have not identified to the Foundation, as this was never a requirement that was set in stone. There were some plans to force every OTRS agent to identify to the Foundation in February 2011, but they don't seem to have been put into action, in the end. odder (talk) 22:31, 14 October 2013 (UTC)

> > When I joined OTRS in September/October 2012 I did not have to identify, though I did a few months later for my OS flag. --**Rschen7754** 23:11, 14 October 2013 (UTC)

> > > Hi MF-W, odder, and Rschen7754. I know that you have seen this related discussion, but I wanted to point out to others who might be following this thread that the OTRS question is still being discussed and we'd love to hear more opinions about whether OTRS members should be included. As for other types of community members who may not have yet identified, this clause is meant to cover anyone who has access rights who may have not known (for whatever reason) that they had to identify under the 2007 policy. Mpaulson (WMF) (talk) 23:37, 31 October 2013 (UTC)

Enwiki ACC

I've notified the enwiki ACC members since this affects us too. Reaper Eternal (talk) 00:46, 15 October 2013 (UTC)

> Thank you Reaper, if you want me to send anything out to them please let me know, it was only my list since I was reminded about them but I won't beleaguer the point if not helpful. Jalexander--WMF 02:21, 19 October 2013 (UTC)

WMF?

It's been a few days and other questions have been answered, but not the more concerning questions above. Does the WMF plan to edit the proposal to address these concerns, or should we be making our decision on whether or not to reidentify based on what the proposal is, since the WMF does not plan to address the concerns above? --**Rschen7754** 01:59, 19 October 2013 (UTC)

> I would encourage you to wait before making any decisions like that. We want to come up with a good policy that as many as possible are happy with. Michelle has been answering questions from her sick bed at home this week (and I imagine you will see a bit more over the next couple days) but we plan to get together early next week in the office to discuss some of the unanswered questions. The consultation is scheduled to last at least 3 more months (there is no hard deadline, if we're not done then we keep going) exactly so we don't need to rush this. Given the experiences with other policy discussions (ToS/Privacy policy etc) I think we can expect that this is just the start of the discussion and edits (both small and major) to the document(s) in the weeks to come. I will be making sure that I stay on top of the legal team to both strongly think about, and answer, all of the concerns being brought up. Jalexander--WMF 02:20, 19 October 2013 (UTC)

> > Rschen's concerns are well justified. Over the last few days, Mpaulson has been addressing a lot of minor concerns that don't require pretty much a complete rewrite of the policy, and has even implemented one edit to the policy. At the same time, all of the major concerns have been completely ignored. It just feels like the WMF wants to implement it very close to its current form, and is consequently ignoring any complaints which would require a big change. Thanks for clarifying that these are being looked into and will be addressed... if that's what you're saying. Ajraddatz (Talk) 02:31, 19 October 2013 (UTC)

> > > That is indeed what I am saying :). I know that people are frustrated by a bunch of pieces and we are in no way trying to ignore any of it (I can't think of anything that isn't up for discussion) Jalexander--WMF 02:34, 19 October 2013 (UTC)

> > > > I've appreciated the way the largest questions have been thoughtfully addressed. Thanks to the legal team for the thorough and ongoing replies. --SJ talk 21:55, 24 October 2013 (UTC)

> > > > > Hi Rschen. I just wanted to follow and let you know that we're responding to a lot of the big issues this week. Many of these responses are clarifications and ask for further response from the community. Once we hear from more members of the community on key issues (such as whether we should still be requiring identification at all, submission of identifying information rather than copies of identification documents, what kind of identifying information would be sufficient, what kind of verification of this information would be needed, what would be an acceptable retention period for such information, etc.), we will start making proposed edits based on the feedback. Mpaulson (WMF) (talk) 23:28, 31 October 2013 (UTC)

- **Note:** Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:03, 3 December 2013 (UTC)

Identification

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:05, 3 December 2013 (UTC)***

Would the photo ID have to remain valid for the duration of the time the rights are held? --**Rschen7754** 19:48, 14 October 2013 (UTC)

> Good point. Surely the WMF also needs to be notified on address changes etc. to ensure that all required data is always up-to-date! --MF-W 22:07, 14 October 2013 (UTC)
>
> > Great point, Rschen7754 & MF-W! We will add "inform the Wikimedia Foundation of any change to their name, address, or email address within a reasonable time following such change" to the identification section of the policy draft. We will hold off on addressing the photo ID remaining valid throughout the duration that the rights are held until we hear more input about whether copies of photo identification should be held at all. Thanks! Mpaulson (WMF) (talk) 22:50, 31 October 2013 (UTC)
> >
> > > Lol. I said this as a joke of course, in order to mock the ridiculousness of the proposal. The change (https://meta.wikimedia.org/w/index.php?title=Access_to_nonpublic_information_policy&diff=6222708&oldid=6222528) of course only adds to the ridiculousness, so you could as well already "address the photo ID remaining valid" while there is finally the option to discuss sth useful like whether copies of photo identification should be held at all. --MF-W 11:59, 8 November 2013 (UTC)

Change of identity information

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:05, 3 December 2013 (UTC)***

What would be done in the event that the identity information of a person changes? I'd like a policy covering the following points:

- For those who currently hold access rights, documentation must be submitted; for those who previously held access rights (and whose information is still retained), documentation may be submitted.
- If a new ID document is submitted, WMF's copy of the old ID document will be discarded; if the submitted documentation of change is not an ID document on its own, both it and the old document will be retained until (if ever) a new ID document is submitted or the retention period expires.
- If a person who previously held access rights submits a new document, this does not reset the retention period.

I'll admit I'm not entirely sold on whether a copy of ID documents should be retained at all, but if it is, a policy on changing information is necessary. (As an aside, is there a reason the name of the policy is being changed from "access to nonpublic data" to "access to nonpublic information"?) MaxHarmony (talk) 21:03, 14 October 2013 (UTC)

> Hi MaxHarmony! These are all excellent points. I will make some proposed edits to the policy draft for your review. As for the name change, it was primarily for consistency. In the new privacy policy draft, the term "information" rather than "data" is used. Thank you for taking the time to make these suggestions. Mpaulson (WMF) (talk) 17:58, 18 October 2013 (UTC)

Valid for Supportteam-members with access to OTRS-queues?

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:06, 3 December 2013 (UTC)***

Does the section: *"Community members with access to any tool that permits them to view nonpublic information about other users"* include supportteam members with access to OTRS-queues?

If yes, what is the rationale of requesting to store a copy of the picture ID Documents and residence for Supportteam members. Best regards --Neozoon (talk) 23:16, 14 October 2013 (UTC) (identified member of the German Supportteam)

> Just a note that there is a discussion above here at OTRS_volunteers where Michelle commented and asked for some thoughts. This is something that is currently being discussed internally and having opinions here is very important in my opinion. In general we currently tell people as they join OTRS that they may have to identify (but have not been enforcing that), whether the policies should be merged or not is something I think should be discussed along with this policy as it should be addressed in it (even if it's an exception. Jalexander--WMF 00:25, 16 October 2013 (UTC)

Why a 3-year post removal retention period?

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active (including too the retention period) I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:06, 3 December 2013 (UTC)***

I can see retaining ID information for a period of time, perhaps 6 months to a year after removal (voluntary or involuntary), with a clause stating that information will be retained longer if there is an ongoing internal (WMF/Ombud) investigation; however, three years seems awfully long. I bear in mind the significant number of people with this level of access who are comparatively transient (e.g., students, those whose work requires travel or moving), so three-year-old data is probably fairly useless. Can we have an explanation of where the 3 year period came from? Risker (talk) 23:18, 14 October 2013 (UTC)

> Michelle? --MZMcBride (talk) 22:36, 20 October 2013 (UTC)
>
> > Hi Risker and MZ. Sorry about the delay. I had pneumonia and am playing a serious game of catch up this week. The reason why we had decided on 3 years is that when discussing potential periods for retention with the Ombudsman Commission, it seemed possible for an investigation concerning the actions of a community member with these kinds of access rights to still be ongoing 2 years after the community member in question had resigned their rights. This could be the case in a particularly complex investigation or one that did not come to the attention of WMF or the Ombudsman Commission until after the community member resigned their rights. That said, I understand that 3 years can be perceived as a long time and if the community believes that investigations of these kinds are all but rarely resolved in a shorter period of time than 3 years, I'm certainly open to hearing what they believe is a more reasonable length of time. Mpaulson (WMF) (talk) 21:34, 22 October 2013 (UTC)
> >
> > > A maximum reasonable time I think would be 6 months after removal, and extended for an investigation as Risker suggests. At the same time, I don't see what benefit holding information for investigations would give anyway, and this gets at the complaint that this change is a solution looking for a problem. Are the functionaries so rogue and out of control and abusing of their rights that this has lead to multiple cases recently where having their personal information on-file would have solved the case, or at least allowed WMF to sue them? If the entire motivation for this change is so that WMF can sue all the crazy rogue functionaries, then all the rhetoric here about us being really trusted people whose input is desirable is just a farce. On the one hand, we're the cream of the crop (or so you'd think reading things like "community members who are in the valuable roles"), but on the other we're so naughty and prone to frivolous revealing of the confidential information we have access to that they need to keep our personal information so they can sue us. I think that before any more responses are given on specifics, the WMF legal team needs to finally answer the question of why this change is happening. Ajraddatz (Talk) 22:23, 22 October 2013 (UTC)
> > >
> > > > Hi Ajraddatz. Thank you for your input on what you believe to be a reasonable retention period. What do other community members think?
> > > > As to your other comments, please see the posting I have done on why we believe a change is needed and the possible solutions that we think we could pursue. We would love to hear your feedback on this issue. We recognize that this is a sensitive topic, but please believe that we are trying in good faith find solutions that work for the community -- and figuring out what's best involves a lot of discussion with the community, which is why we are having this discussion. Mpaulson (WMF) (talk) 22:11, 25 October 2013 (UTC)
> > > >
> > > > > I think that's fair. I think someone suggested keeping the real name around for longer due to certain past cases, and I don't have a problem with that either. --**Rschen7754** 22:15, 25 October 2013 (UTC)

There are different answers for me depending on who is holding the records and for what clear purpose. For community investigations, zero, these are legal records I don't see why community bodies, which according to our long history have proven insecure, should hold them, when there can be no legally binding investigation by definition. For the WMF, zero, as again this is a system subject to unspecified future changes or a general loss of corporate memory (refer to many, many cases of private records of all sorts turning up in skips after company changes from wind-up through to office redecorating meaning someone lost track of the filing cabinets). If legal records of identity were held on an escrow contract of some sort, where a leak or data breach means the holder will pay *handsome* compensation out of their data protection insurance (a requirement on Chapters for payment processing as I recall), then perhaps a period of a year might be perfectly reasonable *if* the escrow contract specified the records can only be released as part of a subpoena and the records had to be retained in the country of residence for the person they identify. --Fæ (talk) 23:12, 25 October 2013 (UTC)

sharing info to someone with an nda

The following discussion is closed: ***closing this off for now given the large amount of changes since it was created and the more current discussion about the release to 3rd parties below. Will archive in a couple days unless reopened.***

Perhaps I misumderstand, but I find the following concerning: "*The Wikimedia Foundation will not share submitted materials with third parties, unless such disclosure is (A) permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department;...*"

Does this mean that the foundation could theoretically give this info to an advertising company provided they signed an nda of some sort? What sort of nda are we talking? As far as I can tell there is no requirement that said nda is a restrictive one, any old nda the foundation legal department likes will do. This seems kind of scary to me.

> Good question, Bawolff. We could say instead: "(A) permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department **consistent with the privacy policy**". That would limit transfers for uses set out in the privacy policy, which does not include, for example, advertising. If that works for you, we will make this change. Geoffbrigham (talk) 20:04, 1 November 2013 (UTC)

On the subject of passwords, I'd like something a little stronger than that - encrypted with whatever the current best practise is for crypto, with what specific encryption is used. Is there logging? Do different people use different passwords? How many people have access? Is it stored on a non networked computer? (Perhaps the entire security model is out of scope for this document, but I'd like assurances its not just a dummy password with the file on the hard drive being unencrypted. Bawolff (talk) 02:14, 15 October 2013 (UTC)

> Another good question. Our thinking is to have the same level of security that we might use for electronic employee records. But, to be honest, we will need to research this a bit more once we have an idea on how the community would like to proceed. We offered another alternative below where we would not need to store such information. Thanks for your inquiries! Geoffbrigham (talk) 20:15, 1 November 2013 (UTC)

Some food for thought

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active (including too the retention period) I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:22, 3 December 2013 (UTC)***

I'd like to offer some food for thought as to what would personally make me comfortable enough to re-submit my id. This is just my personal idea, and others will have different ideas. I feel the wording of the proposal and the way it has been brought about is very disappointing and a bad start, but I think I understand the underlying reasoning, and agree with it to a certain extent.

I first will seek to explain what is so scary about what's currently in the proposal:

- " Physical copies of submitted materials will be kept in locked cabinets designated for this purpose" -- sorry, if I send you a photocopy of my passport, I'd rather not it be in Philippe's locked cabinet. I want it in an actual, serious safe. And I want to know that only Philippe and Geoff have the combination for it.

  > We are open to different security options, including a safe. But I do want to note that a locked cabinet is the same level of security given to the highly sensitive employee material. What do other community members think about the level of security for physical storage?
  > As for who has access, we can limit the people who can access it, but we should avoid naming specific people rather than offices because this policy (if adopted) should ideally apply regardless of whomever holds Geoff or Philippe's role and take into account what happens if both of them are out of the office. Perhaps something along the lines of "access to these materials will be limited to staff members of the Legal and Community Advocacy department of Wikimedia Foundation"? Mpaulson (WMF) (talk) 21:07, 31 October 2013 (UTC)

- "Electronic copies of submitted materials will be protected by passwords or other electronic protections in files designated for this purpose." This part feels like a bad april fools' joke. I send you a scan of my passport, encrypted with PGP and you just stick it in a zip file with a password that anybody can open with Elcomsoft? Please. If you want to retain electronic copies of our IDs, you need it encrypted, in an offline system and audited by reliable third party firms. And again, only Philippe and Geoff can access it.

  > We intend on giving any personal information submitted or held electronically as a result of this policy draft the same level of security that we give to the personal information of WMF employees or our financial information. Mpaulson (WMF) (talk) 22:17, 31 October 2013 (UTC)

- "The Wikimedia Foundation will not share submitted materials with third parties, unless such disclosure is (A) permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department; (B) required by law; (C) needed to protect against immediate threat to life or limb; or (D) needed to protect the rights, property, or safety of the Wikimedia Foundation, its employees, or contractors." No, if I send my ID, the WMF can only disclose it following a court order, the end.

  > First, I think it's important to note that there are circumstances that would warrant disclosure that are required by law that would not involve a court order. For example, if we receive a legally valid subpoena or warrant, we would be required to comply with it. (Of course, if we had reason to believe that it was not valid, we would challenge it.) This is why we said "required by law" in subsection (B) as opposed to "compelled by a court order".
  > I'd also like to understand why you are opposed to disclosure if a volunteer threatens immediate harm to another person and identifying information is required by the authorities to prevent such harm (covered by subsection (C)). Could you clarify your position? Similarly, I'd like to better understand your objection to subsection (D), which would allow us to disclose information about a volunteer to proper authorities if they, say, purposefully planted any viruses, malware, worms, Trojan horses, or malicious code that could harm our technical infrastructure in violation of the Terms of Use or that could expose the personal, nonpublic information of other users. Mpaulson (WMF) (talk) 21:43, 31 October 2013 (UTC)

- "Sometimes, the Wikimedia Foundation or a user community committee will need to contact a community member who formerly had access rights about his or her usage of those rights. For example, the Arbitration Committee may need to complete an ongoing case they are examining or the Wikimedia Foundation may need to notify you of receipt of a legal document involving that community member." No, if I give you my address, it cannot be disclosed to some random arbitrator from enwiki because they wish to bring a case against me because I don't fill my edit summaries. It should only be used by the WMF's Counsel, after the WMF has been sued because I disclosed confidential informations that damaged a third party to point the judge to me as the person that should be sued. Nothing else, ever.

  > You may be interested in a related discussion addressing this very issue. Mpaulson (WMF) (talk) 21:13, 31 October 2013 (UTC)

- "For this reason, the Wikimedia Foundation retains submitted materials for a period after the community member ceases to have access rights. Submitted materials will be maintained as long as the community member who submitted the materials has access rights, plus up to an additional three (3) years." You do not need 3 years, so you shouldn't have 3 years. 6 months, sure, 3 years, nope, no way.

> We are open to altering the retention period. Would you mind reading the retention period thread and letting us know what period you think would be reasonable in light of what's written there? (I would really appreciate this as I'm trying to move all comments regarding data retention to that thread so that it's easier to track and easier for everyone to see the considerations involved in determining what the data retention period should be.) Thanks in advance! Mpaulson (WMF) (talk) 23:06, 25 October 2013 (UTC)

- "If a community member ceases to have access rights, he or she should notify the Stewards. The Stewards will inform the Wikimedia Foundation and the submitted materials will be destroyed by the Wikimedia Foundation in a timely manner following the three (3) year period." In no way should us, the Stewards, have anything to do with this stuff. Anything that has to do with IDs or related should be handled by WMF personnel trained in the handling of personal data and on a need to know basis. Said personnel should figure out when it should be deleted, not us.

> Please see Philippe's response on this issue below. Thanks! Mpaulson (WMF) (talk) 22:18, 31 October 2013 (UTC)

- "Community members with access rights may submit the required Identification and Confidentiality materials to the Wikimedia Foundation electronically. Hard copies may be submitted on a case-by-case basis." No, it has been long-standing practice to accept ID in the forms most convenient to the user, and this should not stop. Especially given a locked cabinet is better than a zipped and password protected file, which are the options as it stands.

> We would be fine with that change (assuming that identification documents are submitted at all, a decision that is still pending as we are still waiting to hear more from the community on that matter). Mpaulson (WMF) (talk) 21:56, 31 October 2013 (UTC)

- But above all, there is no reason for the WMF to keep a copy of my passport. Zero. I understand that you need to know who I am and where I live in case you have to sue me, that is okey. But once you saw my passport and established that I am who I am, you only need to keep this information in your archives, you do not need a copy of my id. Be them encrypted offline archives or locked safes.

> Again, we are interested in hearing from more members of the community on this matter. Would the community be more comfortable if we only retained the identification information rather than copies of the identification documents themselves? Mpaulson (WMF) (talk) 21:56, 31 October 2013 (UTC)

- Somebody suggested a bank vault. I actually like that idea. Keep a copy of my name, username and address in a bank vault or if there's a reason why it really can't be there, an outside law firm offices' safe. You don't need anything else.

> We are actually pretty uncomfortable with this possibility. We have some serious concerns about the potential for disclosure if the information is held by third parties. We are pretty vigorous about pushing back on requests for user information when we believe that such requests are not legally valid. We honestly cannot say the same about more traditional institutions such as banks. Mpaulson (WMF) (talk) 21:56, 31 October 2013 (UTC)

I know that there are some folks that cannot live with the IDs being retained, or even their name being retained. I respect them, but that is not my case. I am willing to let the WMF have my name even in perpetuity if they wish. I am not willing to let the WMF keep my passport scan in a zipped file or a locker. I think functionaries deserve more than that, and the wording of this proposal is unacceptable, especially given when this was raised before the OTRS community had grave objections to the locker/cabinet. I know you can't win all of the people over on retaining data, but this attempt is not going to win anybody over period as long as it is construed this way. I am still shocked that anybody at the WMF would be so out of touch to think that a locked cabinet or a password-protected archive was anything but a joke. **Snowolf** How can I help? 02:38, 15 October 2013 (UTC)

> I would like to highlight my experience of the reality of fraud with regard to passports. *Several years ago an Australian friend was looking for an apartment in Paris, knowing his boyfriend rather well, I acted as his UK reference for a money transaction in London for a deposit of more than 1,000 euros for the lady that was looking to re-let her lease. It was a scam and he lost his money (this is now recognized as a 'classic' scam but it was new back then). With the UK police, I investigated the background and key to the scam was a passport scan that had been doing the rounds with scammers for some time. I managed to contact the lady whos passport it was, and she was the victim of an earlier scam and her identity was being used for multiple later crimes, she put me in touch with a fraud detective in Interpol who was tracking all instances of this fraud. Unfortunately once your ID is compromised this way on the internet, it becomes impossible to put the genii back in the bottle, her scanned passport page (with real name and address details) can be still be found on scam websites and is no doubt still being used to commit fraud in her name.*
> +1 for Snowolf's suggestion that **any ID material is not held by the WMF office, but held in escrow** using a service off-site and only accessed after a direct legal requirement to do so, rather than a request from some unpredictable committee of volunteers who are unlikely to be able to prevent emails or material being "leaked" if it turns out to be of interest to the newspapers. These services range from very cheap to free, from banks and legal firms. --Fæ (talk) 08:20, 15 October 2013 (UTC)
>
> - Good idea, however I can imagine also that some community members could feel LESS safe with a third party involved. Pundit (talk) 06:04, 16 October 2013 (UTC)
>
> > We're still working through some of the points that were raised here, but I'd like to respond to a couple of them: first, regarding having the info held by a third party firm - I think that's a bad idea. If we store it in house, my understanding is that we are, broadly, covered by attorney/client privilege for doc here. (Disclaimer, IANAL).

Stewards - It's been raised that the process as laid out here adds work to the stewards (given that they they have to notify us). I can see the point. I suggest that we remove that line, (*edit: it has been removed.*) and staff will monitor the logged actions for what we need. Philippe (WMF) (talk) 21:59, 25 October 2013 (UTC)

> Hi Snowolf. Thank you for your thoughtful comments. We are going to try to address each of your points in turn, in-line. We will get to all of them, but I just wanted to let you know that the responses may come piecemeal because we're trying to address issues throughout the discussion page by subject. Just didn't want you to think that we are only intending to address some of your concerns. Mpaulson (WMF) (talk) 23:01, 25 October 2013 (UTC)

Purpose

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active (including too the retention period) I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:23, 3 December 2013 (UTC)***

This page, nor the wikimedia-l thread, nor the blog post, say anything about exactly what problem this new policy would solve. The current system works well and I see no reason to change it. I think the new one is going to be purely inconvenient for our existing functionaries, mainly per Snowolf.--Jasper Deng (talk) 04:25, 15 October 2013 (UTC)

> I have to agree here. What is the problem with the current system that requires the WMF to give out my address to all and sundry? Chase me ladies, I'm the Cavalry (talk) 13:37, 15 October 2013 (UTC)
> Also, just because other sites might do this doesn't mean we should.--Jasper Deng (talk) 04:54, 16 October 2013 (UTC)
> I agree as well. There is nothing here that solves a problem. All it does is cause new ones. -Djsasso (talk) 16:43, 21 October 2013 (UTC)
>
> > Hi All. You may be interested in reading this post about this very topic. I would be very interested in hearing your thoughts. If you get a chance, please let me know what you think on that discussion thread. Thanks in advance! Mpaulson (WMF) (talk) 22:24, 25 October 2013 (UTC)

Purpose of retention for address

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active (including too the retention period) I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:24, 3 December 2013 (UTC)***

Thanks for publishing this draft and getting us involved. In particular I think it's good that you've not required that the government-issued identification have your address on it, as some countries like the UK do not have an identity card scheme and as I don't drive my only government-issued photo ID is my passport which doesn't have my address printed on it. However, in spite of me applauding this, it does raise a few questions for me.

1. **Verification of provided address**. It seems that with no way of checking the address that the person provides, there is no way of verifying the address that's given. Is this just an accepted risk you're taking?
2. **Purpose of requesting address**. In light of the fact that the information supplied may be completely fictional, I'm not sure what the purpose of requesting it is. Some clarification may be helpful.

--Deskana (talk) 09:35, 15 October 2013 (UTC)

> Some websites, such as couchsurfing, use/used postcards with a code for address verification. If they were accompanied by some wiki merchandise, many users would not mind :) This is apart from the discussion whether an address is actually necessary for the WMF to have. Pundit (talk) 06:02, 16 October 2013 (UTC)
>
> > Hmmm..... interesting Jalexander--WMF 02:42, 19 October 2013 (UTC)
> >
> > > Hi Deskana and Pundit! Indeed, these are some great ideas. I would be interested in your thoughts about the general requirement of submitting an address. Mpaulson (WMF) (talk) 20:53, 31 October 2013 (UTC)

What about stolen accounts?

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active (including too the retention period) I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:43, 3 December 2013 (UTC)***

What will happen if one of these "highly-identified" accounts will be stolen? Just some days ago there was a potential security breach when thousands of hashes has been made almost public on WMF labs. So the owner will be legally charged with every misuse of his stolen account? I use quite strong passwords and secure user-side devices/software but still my account can be forced in every other point of the chain bringing me to WMF. So, from an "investigative" point of view, identification via IP will always be needed, so why do we need to store IDs? You should also be aware of the revolution in security measures WMF must to take since another "labs leak" will expose the Foundation to serious legal threats by her own users so I must presume WMF

will completely re-design their software and their software development process. My bank and other organisation giving me a legally binding online identities signed strong strong agreement assuring me I won't be charged for their faults nor my good faith faults, will WMF do the same? --Vituzzu (talk) 10:58, 15 October 2013 (UTC)

Yes, this is the point I was trying to make, but you put it more clearly :) --**Rschen7754** 04:25, 16 October 2013 (UTC)

@Mpaulson (WMF): are there plans to clarify the wording (I think it was the confidentiality pledge actually)? Personally I would suggest something like "in cases of willful intent to violate privacy, or gross negligence", but IANAL.
--**Rschen7754** 20:11, 30 October 2013 (UTC)

Hello @Rschen7754: and @Vituzzu:, thank you for this question. This policy and the Confidentiality agreement for nonpublic information applies to "you" -- the person using the account. Is there another section where this could be clarified? A user should not share his or her password (under the Terms of use), but it is not a violation of these policies if a user's account is stolen (through no fault of the user). In practice, a user will have his or her technical privileges revoked if it appears that his or her account has been compromised. For example, a steward under the CheckUser policy may remove a checkuser's access. The intent is to ensure that checkuser tools are not used by someone who was not selected and entrusted by the community. Thanks Stephen LaPorte (WMF) (talk) 20:15, 1 November 2013 (UTC)

Board of Trustees

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active (including too the retention period) I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:44, 3 December 2013 (UTC)***

I'd like to read some words from the Board about this change. --Vituzzu (talk) 11:12, 15 October 2013 (UTC)

On a similar note, has the Ombudsman Commission taken a stand here on this specific proposal? Pundit (talk) 06:06, 16 October 2013 (UTC)

Hi Vituzzu and Pundit! The Board is, of course, welcome and encouraged to join this discussion. And the Ombudsman Commission actually helped us craft the concepts included in this policy draft and provided useful feedback during the drafting process. Mpaulson (WMF) (talk) 23:17, 17 October 2013 (UTC)

That was my understanding, but I wanted this to be clear. Pundit (talk) 06:57, 18 October 2013 (UTC)

Michelle: it's a bit strange to read that the Board is "welcome and encouraged to join this discussion." This policy has no effect unless the Board says so. The Board is quite a bit more than welcome and encouraged to join the discussion... the Board should be actively leading it. --MZMcBride (talk) 22:32, 20 October 2013 (UTC)

Heh. Surprised? Theo10011 (talk) 23:28, 23 October 2013 (UTC)

MZMZ - A global policy such as this would have to be discussed and approved by the Board to take effect. But that does not mean that all public discussion must be led by the Board. LCA in particular is designed to coordinate public discussions about their work, including any policy recommendations they make to the Board -- such as is happening here. In those cases there are reasons not to have the Board jump in with comments before a public discussion, since the hope is to reach an understanding of appropriate community norms, and we are sometimes derailed by threads that try to oppose board and staff comments [rather than empowering the community to draft a policy it finds appropriate in the first place].
The Board has not revisited this policy since 2007 - see also this comment from 2011 when it was last being reinterpreted. Members of the Board are reviewing these policies and proposals at the same time as the rest of the community, thanks to this public discussion; but we don't get to weigh in "as a Board" until there is a recommendation before us. Which, given the quality of the legal-community discussions in recent years, I am certain will be an excellent one. --SJ talk 19:47, 24 October 2013 (UTC)

Vituzzu - the current policy on how users identify to the WMF, and for what reasons, is vague on how identification is implemented. I do think that this should be covered more clearly in an "access to private data" policy -- at least to be clear about current practice. --SJ talk 20:03, 24 October 2013 (UTC)

Michelle - I appreciate your sentiment. It is hard for Board members to join such a discussion individually, since our primary position in these cases is strong support for staff in engaging directly with the community; and since our personal views are often mistaken for Views of the Board. That said, I have shared some brief personal thoughts below, as a community member and not a Board member, in areas where clarification would help me.

Thank you for clarifying, SJ. Your thoughts are always appreciated! Mpaulson (WMF) (talk) 22:20, 24 October 2013 (UTC)

exact scans vs. data

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active (including too the retention period) I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 21:45, 3 December 2013 (UTC)***

I understand that WMF may need to be able to link the special trust accounts with actual people. Stewards, checkusers, oversighters have tools which technically allow privacy breaches on all other members of the community and it is only natural, that the safety and privacy of everybody wins with the right to privacy of those tool holders. I'm curious about one thing, though. Several members of the community expressed concern about their ID scans being kept by WMF simply because such IDs, if anything goes wrong, may be used for identity theft. I'm wondering then whether WMF indeed needs full ID scans, or is a basic confirmation of one's identity (with typing a name, date of birth, and possibly a declared or verified address into a database) not a better solution? Pundit (talk) 06:10, 16 October 2013 (UTC)

> If the problem here is that we need a legal record of verification, then I would have far fewer concerns in proving my identity to a local notary public (a solicitor on my high street charged me £5 the last time I did this) and then providing the approved relevant scan to an escrow facility in my country (again, these are cheap as chips or even a free service that the WMF bank or regular solicitors could provide). As for the security of a third party, if it is a bank or a solicitor's secure facility, then the level of insurance/compensation available in case of fraud would be far, far higher and more reliable than the WMF can provide. As a solution this reduces risk of fraud for both volunteers and the WMF, or the catastrophic case where volunteers are being forced to sue the WMF for compensation after a disgruntled employee (or someone else hanging around the WMF not-as-secure-as-a-bank offices) does something stupid. --Fæ (talk) 07:11, 16 October 2013 (UTC)
>
> > (Btw notary public exists only in Common law)
> > Actually I contested the whole process of association between accounts and identities since, from a legal point of view, we cannot give any legal warranty about account strength thus an IP check will always be needed. --Vituzzu (talk) 12:34, 16 October 2013 (UTC)
>
> I don't think we're tied to keeping full IDs. We'll have to think on the option some more, to make sure we're not missing something. Would it reduce your other concerns if we did that? Importantly, would you be OK with us asking for things that might not be on all IDs (such as addresses)? -LVilla (WMF) (talk) 22:49, 25 October 2013 (UTC)

Draft confidentiality agreement

The following discussion is closed: ***close, looks like the discussion is finished/stale, will archive in a couple days unless reopened. Jalexander--WMF 22:36, 9 December 2013 (UTC)***

For the record we have a draft of the agreement mentioned up already which is also available for discussion. Jalexander (talk) 23:07, 3 September 2013 (UTC)

> So just to begin this part of the discussion, the draft of the agreement says the following: *Authorized Wikimedia community members may include, for example, oversighters, checkusers, functionaries, volunteer developers, and other similar authorized roles.* Can we please clarify what exactly is meant by *functionaries*? Also, including OTRS agents in that list might also be helpful. (I'll try to provide more comments as I read through the text.) odder (talk) 21:41, 19 September 2013 (UTC)
>
> > Hi odder! Thank you for your questions and comments! I've responded to each of your inquiries in-line below for the sake of clarity. I hope that's alright.
> > I agree that the term "functionaries" is a little vague. What we were trying to encompass here was any community member who has been given rights that permit them to access nonpublic, legally sensitive information. However, we realize that different communities may have different terms to describe the group I refer to as "checkusers" or may choose to change the term "checkusers" in the future. Similarly, new roles or access rights may be created in the future by the community that should be covered by this policy, but obviously cannot be explicitly listed. We hoped that the general term "functionaries" would suffice, but we are also very much open to other suggestions.
> > I also agree that adding OTRS agents to the list of users covered by this policy might be a good idea considering that people who write to OTRS frequently include sensitive information about themselves or others. What do other community members think about this? Mpaulson (WMF) (talk) 23:21, 15 October 2013 (UTC)
> >
> > > I do think that you would risk a lot of people leaving, and would also put those in between the ages of 16-18 in an awkward position... --**Rschen7754** 00:27, 16 October 2013 (UTC)
> > >
> > > > Hi Michelle, thanks for your answer. I would simply suggest that you remove the word *functionaries* from the draft, as the number of user groups with direct access to non-public, personal and sensitive information is, I believe, very limited; only oversighters, checkusers, stewards and volunteer developers might have access to such information (as well as members of Arbitration Committees on some projects, but they generally hold oversight and/or checkuser rights already). The term *functionaries* is usually supposed to include administrators (and possibly also OTRS agents); you are already using the phrase *and other similar authorized roles*, which, in my feeling, is enough to cover the possible future scenarios you mentioned.
> > > >
> > > > As far as OTRS members are considered, my intention was only to make things more clear to people; if you want to include OTRS agents, then please do so plainly, and we can discuss the pros and cons of the idea afterwards.

> As an OTRS agent, I have seen many e-mails which revealed very sensitive personal information about people, such as exact (snail-mail) addresses and phone numbers, not to mention real names or e-mail addresses. I think I can say I've had access to more sensitive personal information as an OTRS agent than as a Commons oversighter — so I can understand why it might be good to include OTRS agents in the list, and have them sign the agreement. However, as Rschen7754 rightly points out, this idea has always been controversial among OTRS agents, and many of them might decide to leave if this requirement is implemented, so I think we should try to discuss it in detail. odder (talk) 10:15, 16 October 2013 (UTC)
>
> > What do you think about removing "functionaries" and saying "This policy does not require users whose rights only include the ability to view standard deleted revisions."? Mpaulson (WMF) (talk) 22:16, 25 October 2013 (UTC)
> >
> > > Sounds good to me; thanks, Michelle! I'm not sure how to address Bawolff's point about #Volunteer developers which was brought with regards to the privacy policy, but which is also relevant for the confidentiality agreement—any ideas? odder (talk) 07:02, 26 October 2013 (UTC)

So I read the draft, and here are some more questions:

Comply with the Privacy Policy; the Access to Nonpublic Information Policy; and any other applicable and nonconflicting community policy relating to nonpublic information; -- the community policy part is quite vague. Moreover, it is my feeling that it complicates this point a bit by mixing the requirements of the WMF and community policies; on a related note, I'm not aware of any community policies concerning non-public information, nor do I think that it should be up to the community to decide that. odder (talk) 21:58, 19 September 2013 (UTC)

> The reason why we have included any applicable and nonconflicting community policy relating to nonpublic information is because the Privacy Policy and the Access to Nonpublic Information Policy are baseline protections. Nothing in those policies prevent any particular project's community from creating and enforcing more protective policies with regards to user data. If a community does create such a policy, we would expect community members of that particular project who have special access rights to comply with that community's policies. Does that make sense? Mpaulson (WMF) (talk) 23:21, 15 October 2013 (UTC)
>
> > Yes, it does make sense :-) However, we are still left with the question whether the communities should have any say in the subject of protection of user data. So far, this has been a Foundation prerogative, and I wonder if this change would do us any good. (Just throwing a thought.) odder (talk) 10:15, 16 October 2013 (UTC)

The Wikimedia Foundation may pursue available legal remedies. This sounds *very* scary to me, as if the WMF reserved the right to sue me if I violated the agreement. I would very much appreciate a clarification about what's meant by this sentence.

> I can understand why this clause sounds scary. Believe me, I hope that we never, ever have to use it. The scenarios that this clause is meant to cover are extreme...for example, if a particular person who has checkuser rights uses those rights to access and copy personal information about users without any good reason and then goes on to publish that information in a inappropriate or malicious way, we would want the ability to legally restrain this person from continuing to publish the private information. Mpaulson (WMF) (talk) 23:21, 15 October 2013 (UTC)
>
> > Thanks for the clarification, Michelle, it's very helpful. I can definitely understand why you wanted to include this clause in the agreement. odder (talk) 10:15, 16 October 2013 (UTC)

The laws of the State of California and the United States of America will govern this agreement (without reference to conflict of laws principles). This is also very vague; I believe that people should be informed in detail about what applicable laws there are and what are the exact terms that they will agree to if they sign the agreement. (There are many differences between the various jurisdictions our users are located in, and blankly agreeing to be governed by laws you have no idea about is never a good idea, IMHO.) odder (talk) 21:58, 19 September 2013 (UTC)

> Actually, the reason why we have this clause is to clear up ambiguity, not to create more. We want to be clear that a particular set of laws will govern the way this agreement is interpreted (in this case, the laws of CA and the US). But I don't think it's reasonable or even possible to provide every law that could apply to any particular situation that could arise in relation to this agreement. It would frankly turn this 1 page or so agreement into a treatise with many, many volumes. For example, the statutory and case law covering contract interpretation alone could fill the better part of a library. Mpaulson (WMF) (talk) 23:21, 15 October 2013 (UTC)
>
> > Yes, I'm aware of the complexity and the vastness of the U.S. legal code; it wasn't my intention to make you describe any and all laws applicable to this agreement. However, it would still be helpful for many people to know at least the basic terms of the laws they would agree to if they sign the CA. (There are many questions asked about this part by people below, for instance Vituzzu and Fae, so you can see this is something people are actually concerned about.) odder (talk) 10:15, 16 October 2013 (UTC)
> >
> > > Usually there are small differences among the states in the U.S. on issues like construction of the agreement, damages, and consideration (that is, the quid pro quo of contracts). This article

(http://docs.law.gwu.edu/facweb/gmaggs/maggs-augsburg.pdf) points out some differences among different states as well as Europe. It is a bit difficult to be more specific because it will depend on the facts of each case to some degree, and, in a common law country, the case law in the jurisdiction. Geoffbrigham (talk) 22:03, 25 October 2013 (UTC)

> Thanks for the pointer, Geoff; I'm sure the lecture will be interesting, and I'll try to read more on the subject. odder (talk) 07:02, 26 October 2013 (UTC)

Another part of the agreement got my attention today:

> *(...) your activity or account may be reviewed by other authorized users or the Wikimedia Foundation.'* Does anyone mind explaining the meaning behind *your account (...) may be reviewed* and the meaning of *other authorized users*? I'm especially concerned about a combination of these two parts: *your account may be reviewed by other authorized users*. What does this mean with regards to off-wiki activity such as OTRS? Does this mean that in case of a breach of privacy by a checkuser, other community members with these rights would be able to perform a check on their account? I would welcome an explanation of this point, thanks. odder (talk) 17:50, 7 October 2013 (UTC)
>
> > This means that if there is a good reason to suspect that abuse (or mistaken use) has occurred in relation to a particular account with access rights, the Foundation or other community members with the same rights may review the account and its activity to ensure it is in compliance with applicable policies and that nothing has gone wrong. To be honest, it is unlikely that the Foundation would play this kind of role unless the alleged abuse in question was significant. The more likely scenario is that something unusual happens (or something usual happens and was incorrectly documented) and the other users with the same access rights proceed under their own policies to investigate the matter. Mpaulson (WMF) (talk) 23:21, 15 October 2013 (UTC)
> >
> > > So, to take your example from above, I'm assuming that in case of a checkuser revealing non-public information about another user off-wiki, other checkusers will be able to perform a check on them — is that right? I'm not exactly sure if volunteer community members should be tasked with ensuring compliance with Foundation's policies in cases like that. Also, I'm assuming that in case of OTRS, it will be the OTRS admins ensuring compliance with the various policies (please correct me if I'm wrong). In any case, thanks so much for your answers, Michelle; I appreciate your time. odder (talk) 10:15, 16 October 2013 (UTC)
> > >
> > > > The intention here - as I understand it - is to say that nobody gets to do unreviewed actions. Not Checkusers, not oversighters, and not me. It's a bad idea to have a system where anyone can pull data without creating an opportunity for review of the action. That's why we have logs that are automatically created... my read of this sentence is to spell out clearly that if you Checkuser someone, you should expect that the Checkuser logs will be reviewed. Likewise, if you're oversighting, you should expect that those logs are reviewed. That applies to WMF staff too - I review the logs for staff names, and I know that (for instance) when the English Wikipedia sees a staff member do a checkuser who isn't typical, they review it and notify me. So I interpret the sentence to mean that the actions of the accounts may be reviewed (and, as well, other data about the account (ie, was it logged on then?) if needed. Philippe (WMF) (talk) 21:48, 25 October 2013 (UTC)

OTRS volunteers

The following discussion is closed.

The draft is not very clear about identification requirements for regular OTRS volunteers. For some time now (despite many didn't like it), every OTRS volunteer is supposed to be identified, but in practice past volunteers (and perhaps some of the new too) were not asked to provide identification. Is some clarification of the issue coming? --Nemo 06:13, 4 September 2013 (UTC)

> Agreed imo. Age restriction for OTRS volunteers is set to 16 currently. In my opinion, OTRS volunteers who do not reached at age 18 should be marked seperately in Identification noticeboard. – Kwj2772 (msg) 08:22, 4 September 2013 (UTC)
>
> > That fairly clearly marks someone as "under 18", doesn't it, potentially opening us up to disclosure and child protection issues? Philippe (WMF) (talk) 10:07, 4 September 2013 (UTC)
> >
> > > Then raising the age restriction to 18 would be only option if we're really going to go identification process for OTRS volunteers. Otherwise we can't distinguish them from the identification for checkusers/oversighters. – Kwj2772 (msg) 10:28, 4 September 2013 (UTC)
> > >
> > > > Couldn't we, though? We just have to do it in a more secure area. For instance, we could use a message board that stewards have access to but others don't. Philippe (WMF) (talk) 10:35, 4 September 2013 (UTC)
> > >
> > > Child protection issues for OTRS volunteers?? I might have lost track of what "child protection" term is used for in USA, can you explain? Anyway, whatever you decide please make clear decisions and apply them or it will be again a huge mess with flames everywhere and mass sacrifices of innocents. --Nemo 21:02, 4 September 2013 (UTC)

> If an OTRS volunteer is under 18, they deserve the same protection that we offer anyone else. :) Philippe (WMF) (talk) 21:56, 4 September 2013 (UTC)
>
> > That is? I just said I've no idea what protection you're talking about... --Nemo 12:29, 5 September 2013 (UTC)
> >
> > > Sounds like protection from revealing personal information, which would happen if you put someone's name in a section which specifies that they are younger than 18 but older than 16. Philippe's logic is definitely sound here, but I wonder if the OTRS age should be raise to 18 for consistency and to address the issues raised. Ajraddatz (Talk) 19:07, 14 October 2013 (UTC)

We have been talking internally about whether OTRS agents should be covered by this policy. Currently, only OTRS administrators are covered. There are strong reasons to consider adding OTRS agents given that they have access to nonpublic emails sent by third parties which frequently include sensitive information about those who sent the email (and others). I understand that the current minimum age for OTRS agents is 16. If we were to add them to this policy, we could either make the minimum age 16 for OTRS agents only and keep the rest at 18 or the OTRS agent minimum age could be raised to 18. What do others think about these ideas? We've love to hear the community's thoughts on this subject. Mpaulson (WMF) (talk) 23:28, 15 October 2013 (UTC)

> If you raise the age to 18, then there arises the issue of what to do with those who are between 16 and 18. Any account removals would be publicly logged, and people could guess their age that way. --**Rschen7754** 02:41, 16 October 2013 (UTC)
>
> > Fascinating point! If the age is raised, then removing <18 accounts would clearly identify those users as such. However, you couldn't simply grandfather them in - why would the change be needed in the first place if current 16 year olds still had access? Ajraddatz (Talk) 02:54, 16 October 2013 (UTC)
> >
> > > The OTRS admins could simply not remove people <18 from the public list of accounts immediately, but at later times in smaller inconspicuous groups (to make it look like normal fluctuation). --MF-W 14:12, 16 October 2013 (UTC)
> > >
> > > > Now that you've said that, it's probably not going to be a useful way to hide it. You could just get rid of all non-identified OTRS agents with the same reason, not making public whether it was over their legal ability to usefully identify or not. --Krenair (talk • contribs) 23:53, 20 October 2013 (UTC)
>
> If having <18 people hasn't caused any issues for this long, there won't be any issues for two more years. We could just stop accepting new applications from people under 18, and then people who are currently under 18 will be 18 within two years. -- King of ♥ ♦ ♣ ♠ 23:21, 25 October 2013 (UTC)

Regardless of whether OTRS users should be subjected to this outrageous policy, the thing with the Identification noticeboard needs to be clarified. It is untenable that someone might identify for OTRS, be added to the I.N. and then happen to become a CU/OS/steward based on that entry, even though he is still <18. --MF-W 14:12, 16 October 2013 (UTC)

> Yes, but admin actions are generally logged on OTRSwiki. --**Rschen7754** 17:29, 16 October 2013 (UTC)

Speaking as an OTRS volunteer, I have no problem with being identified to this degree - David Gerard (talk) 22:26, 25 October 2013 (UTC)

> Doesn't bother me, either. The age issue is interesting, two questions: (1) how many would this affect as of today and (2) is this to do with the age of legal majority and legal responsibility for handling this kind of informaiton (probably covered already but there's a loooot to read through). JzG (talk) 22:54, 25 October 2013 (UTC)

As an OTRS volunteer, I think it would be even necessary to identify yourself, because there are some volunteers that would have probably have much more professional and warm approach to people addressing OTRS, if they weren't allowed to hide behind pseudonyms. And as someone, who became an admin on a local Wikipedia at the age of 14, I don't really think age is a good measure when it comes to someone's maturity, responsibility, loyalty to community or ability of taking autonomous decisions, but in this case it would probably make sense to restrict it to 18 for legal reasons. Of course, the information should stay of a closed nature (at least I don't want that just about everybody has an access to a photocopy of my id and would definitely reconsider my volunteering if any of these data date would become public) --Smihael (talk) 23:48, 25 October 2013 (UTC)

> I don't have a problem as well with such identification. I am not sure about the legal issues, but if this wasn't severely needed, I would highly oppose such a restriction. Many of the active Wikimedia contributors are school students, and a lot of them become admins before 18. Possibly many of the OTRS agents, too. The important thing is, how far is this necessary; was there any particular case ever when this caused a serious problem? In the case there wasn't, how much would be the possibility of having such a problem in the future? And what's its worst possible scenario for it? I would like to know what the answers looks like before making an opinion --Abbad (talk) 04:53, 26 October 2013 (UTC).
>
> > As volunteer i don't any problem with my identification using a regular system (CU, OS, ...). Alan (talk) 15:16, 26 October 2013 (UTC)

> How about no. I gave my real name and my emailadress. This should be enough. I don't see why people have to send ID's. My privacy is worth more than beiing an OTRS-member which I quite enjoy. Some things are private. Why do they want to know what I look like? Why do they want to know where I live? --Natuur12 (talk) 21:02, 26 October 2013 (UTC)

I just wanted to note something, from a personal PoV (although I am an OTRS Admin I am speaking only on behalf of myself). Ever since May 1, 2007 (https://meta.wikimedia.org/w/index.php?title=OTRS/Volunteering&diff=next&oldid=575099), it has been clearly stated on the OTRS Volunteer application page (although over the years there have been minor tweaks to the wording), that applicants *must* be **willing** to provide identification. The current wording is "Before applying, please ensure that you are...Willing to provide identification to the Wikimedia Foundation if necessary, considering the access to nonpublic data policy". *So this really should not be such an issue for OTRS Agents*. Putting that aside, please remember that the current drafted version, and the drafts we've gotten all along up to this point have never included OTRS Agents under the policy; only Administrators will be affected. Rjd0060 (talk) 01:11, 27 October 2013 (UTC)

> Thus far "providing identification" has only ever meant that copies of the identification would *not* be retained (something that has been reiterated a number of times since 2007), so I'm afraid I don't see the link. **Thehelpfulone** 01:38, 27 October 2013 (UTC)

> > There are users that are concerned with providing the ID all together, before even considering the fact that the information will be retained. But again, the most important thing here ... it isn't set to apply to Agents. Just the Admins. Rjd0060 (talk) 01:44, 27 October 2013 (UTC)

> > > What do you folks think about WMF eliminating the identification process and leaving it to the community to come up with their own standards of identification (consistent with the privacy policy)? I have heard so much objection to identification itself or the various proposed means of identification, so I'm interested in your views to this proposal. Identification without retaining the identifying information is not consistent with the spirit of the Board resolution in my opinion ("Only persons *whose identity is known* to the Wikimedia Foundation shall be permitted to have access to any nonpublic data or other nonpublic information....") So I'm honestly thinking of asking the Board to revoke its resolution and leave to the communities to put into place identification processes that work for their specific communities and needs. Thanks for your thoughts. Geoffbrigham (talk) 22:45, 15 November 2013 (UTC)

Balancing WMF's need to protect itself with volunteers' need to protect themselves

I am an OTRS volunteer. Through OTRS I was given access to (i.e. I handled as part of normal OTRS activities) an email in which I was pointed to a file that had enough information easily steal two people's identities. Obviously the file has since been Oversighted.

In order to get access to OTRS I sent a WMF staff member a copy of a state-issued ID, with some information (anything they didn't explicitly ask for) blurred out, with the understanding that the image would be deleted as soon is it was looked at.

I can absolutely understand the WMF's desire to have a better grip on who is handling the sensitive information on WMF projects. While it's certainly not every day that someone uploads a large chunk of personally identifying information to Commons, it's not entirely uncommon either. But it's important to note that all being an OTRS volunteer did was *point me at the file*. The file was already publicly available, and could have been found just as easily by ordinary Commons users doing cleanup (considering that the uploader had a serious misunderstanding of what Commons was, the file was likely uncategorized, and thus someone else finding it while doing cleanup is a near certainty). Hell, it could just as easily have been found by some random editor clicking 'Random file'.

The vast majority of the sensitive information that OTRS volunteers have access to is phone numbers and email addresses. Celebrities generally have paid staff dealing with OTRS on their behalf, so it's really just the phone numbers and email addresses of random, generally unremarkable (no insult intended) people.

The policy, as written, is unpalatable to a majority of the users that are participating in the discussion. That could be because a lot of people read the and policy and did commented because they have no issues, but considering that there are almost no positive messages about the policy, I would have to say that seems unlikely. On the contrary, right now several functionaries that would be effected by the new policy should it go into effect are threatening to resign over several clauses (parts 3.(b) and 3.(d) mostly).

OTRS already has backlogs that come and go based largely on the availability of volunteers, and it needs a large body of people to keep things running smoothly. If this policy is extended to all OTRS members, some of them *will* resign. I personally will, (and although I'm not active now, at one time I was doing a majority of the photosubmissions queue work). I have to imagine that other people will as well. If too many people decide that they're not going to accept the new policy, it leaves OTRS in a weaker position in terms of timeliness of responses, but does it really lead to a stronger position in terms of security? Is there really any positives? Do we really need to have the names and addresses of OTRS volunteers? I don't think so.

The WMF needs to balance the need to protect the WMF with volunteers' need to protect themselves. The WMF wants to have this information on file in case something goes horribly wrong and it becomes a legal issue, either where the WMF has to declare that personal information it was handling was leaked, or where someone writing into OTRS brings legal action (legitimate or no) against the person that responded to them.

However, by the same token, individual users have to protect themselves. Looking at the Wikivoyage fork debacle, one wonders if more people would be parties to that (frivilous) lawsuit if more people's information was public. If the WMF *doesn't have* the names and addresses of volunteers, it can't *give people* that information. That gives volunteers an added layer of protection from, to put it tactfully, are *unpleasant*. If volunteers don't feel that they have that layer of protection, they're not going to be willing to handle the angry people that write in threatening to sue the WMF and everyone that edited some article or another, and they're not going to be willing to handle the people that seem of questionable grounding.

Ultimately, I don't feel that there is enough of a benefit to the WMF, or enough of a risk that the WMF needs to protect against, to warrant having OTRS volunteers as an included body for this policy. Sven Manguard (talk) 20:42, 31 October 2013 (UTC)

> Thanks Sven Manguard. What do you think of our proposal to eliminate the identification process? Geoffbrigham (talk) 00:55, 6 November 2013 (UTC)

- **Note:** Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 18:49, 9 December 2013 (UTC)

Signing the pledge and resulting liability implications

The following discussion is closed: ****Note: Given how the changes made closing this has done, will archive in a couple days unless reopened. Jalexander--WMF 19:12, 9 December 2013 (UTC)***

Having trusted users sign a pledge in association with their full legal identity, appears to be an enforceable contract between the legally identified person and the Wikimedia Foundation. This would appear to make the trusted user liable for damages in a case raised against the WMF for any actions the trusted user may have been involved with, or thought to be involved with, whether they were paid for their time or not. Three questions:

1. By signing this contract, exactly what potential liability does the trusted user take on for the consequences of their actions and is the liability limited or unlimited?

2. Would the WMF be obliged to provide legal identities for trusted users so that a complainant could name them in a legal case of damages?

3. If there is a risk of liability, will the WMF provide liability insurance that will be sufficient to cover expenses or damage claims in any future legal action with respect to any actions a volunteer might have made as a trusted user? I note that in the UK, such insurance is commonplace for charities where volunteers may take on operational duties as well as employees. Wikimedia UK gives its volunteers this form of liability insurance when acting for the charity, and the volunteers have access to the policy to review if they wish.

--Fæ (talk) 23:55, 14 October 2013 (UTC)

> I'm not a lawyer, but I think the question of whether its enforceable or not (and to what extent) is not super settled. I'm sure there is a category of law out there dealing with "contracts" with unpaid volunteers, but I think generally speaking for an agreement to be binding there needs to be a degree of consideration involved. It's a similar issue as applies to non-disclosure agreements between entities where the NDA is the only tie. In this case, the information probably has no commercial value either, so... the agreements are basically a promise to tie you up in court and cost you money with legal fees, that's about it - and even *that* is only for parties within the U.S. Good luck enforcing a non-disclosure agreement against a checkuser in Russia or Italy or China. (edit to add: in other words, its all paper covering the WMF's ass and not much more.) Nathan T 00:11, 15 October 2013 (UTC)
>
> > I can understand your concerns, but I'm comfortable with the language of the agreement for our purposes. Consideration usually needs to be only minimal, and frankly resort to enforceability would only be reserved for really exceptional cases; our primary objective is to spell out the clear expectations of the community in the handling of non-public user information, so people comprehend their responsibilities. Courts may limit liability according to the circumstances, but I would imagine that the most common legal remedy would be a declarative judgment to comply with the agreement or injunctive relief not to disclose further private information. I don't understand the question about "legal identities." WMF may be required to disclose information in its possession if it received a legally-valid subpoena consistent with the privacy policy - though we aggressively resist subpoenas that are overly broad or otherwise legally deficient. As a matter of practice, we also notify users when possible relating to subpoenas requesting their user information. See draft privacy policy. Since the volunteers in the community do not act on behalf of WMF, we would not provide insurance, though we do have available for administrators the Legal Fees Assistance Program when applicable. Also we have suggested an alternative approach below that addresses some of the concerns you mention here. Take care. Geoffbrigham (talk) 19:53, 1 November 2013 (UTC)
> >
> > > @Geoffbrigham: Well, the problem is that a lot of volunteers are not comfortable with the language. Our signing this pledge would basically give our legally binding consent for the WMF to file a suit against us for damages. I've interacted with enough WMFers to know that you would only pursue legal action when necessary; however, we don't know who the WMF will hire down the road, and we would hate to be wrong about something like this. Adding additional language to clarify the scenarios in which WMF would file a suit would go a long way. Speaking for myself, this is the dealbreaker for me - I might not be happy about the rest of it, but I might go along with it anyway; yet the liability issue and my possibly having to take out insurance just to be a steward/CU/OS or whatever is problematic. --**Rschen7754** 20:17, 1 November 2013 (UTC)
> > >
> > > > Thanks for the clarifications Geoff. I take from your statement that:

1. Despite insurance being mentioned elsewhere on this talk page, the WMF does not actually insure any volunteers or other trusted users and has no intention of doing so, even where WMF projects rely on these volunteered services. I note that some Chapters do insure volunteers when acting in roles that would otherwise have to happen through paid project contractors, and this does happen as standard good practice for a large proportion of other charities that rely on volunteers to deliver charitable services to their beneficiaries.
2. You understand my concerns, but you remain comfortable with the policy as it fits your purposes.
3. The legal document has the primary objective of spelling out expectations for handing non-public user information. That it now creates a mechanism for legal enforcement, such as a volunteer being sued by the WMF for indefinite sums of money, seems a secondary concern.
4. The WMF shall pass on legal identities of volunteers in response to any valid subpoena from any party.

--Fæ (talk) 23:34, 1 November 2013 (UTC)

> Hi Rschen - so I guess I need to understand better what you think is acceptable. As we suggested above, we could create a regime without identification, which would alleviate some of the above concerns. If that is not the approach that the community wants, we could try to limit the type of legal relief - such as a restriction to injunctive relief. Or we could allow monetary damages up to a certain amount ($30,000?) or only with a significant level of legal intent (something like "willful" disclosure). The challenge is that we cannot anticipate all situations. The one "test" question I ask myself is if a checkuser sells nonpublic information for personal profit, what remedies would the community find appropriate? I would be most interested in your thoughts on this. Thanks. Geoffbrigham (talk) 08:55, 6 November 2013 (UTC)
>
> > "Willful disclosure" would be fine by me, or "gross negligence" (choosing a password like "password" for example, or allowing someone to borrow your steward account and that person does bad things with it, etc... when the holder of the advanced rights clearly should know better - though I can see how that might be a harder line to draw). I personally don't see the same issues with injunctive relief, since at least according to my understanding, any financial impact would be minimal (as long as you don't break the agreement). I don't think many people would have problems with the WMF asking for monetary damages if someone with access to public data purposefully violated someone's privacy to the extent that it caused them real-life consequences (though the case could be made for the person who was outed suing too...) --**Rschen7754** 09:13, 6 November 2013 (UTC)
> >
> > > Rschen - You are correct that injunctive relief would be limited to an order to stop doing something (like "stop your access to and distribution of nonpublic information") - without monetary damage awards. We could limit monetary damages to "gross negligence and willful disclosure." It would mean that a volunteer acting negligently with real consequences to the privacy of others would not pay monetary damages pursuant to the agreement. Does that work for you (and others)? Geoffbrigham (talk) 23:59, 6 November 2013 (UTC)
> > >
> > > > Hi Geoff, you have used some words that I find difficult to interpret, both due to my past professional experience and probably because I am reading them with a UK understanding of English whilst you are writing them from a USA standard. To be honest I worry that many readers here might jump to incorrect interpretations of the specific legal words you are using and so their feedback might end up being based on unwarranted assumptions.
> > > > Putting aside "willful disclosure" (though I think that needs specifying), my understanding of a statement that the WMF will *"limit future claims of damages against volunteers to cases of gross negligence"* is linguistically and legally equivalent to the WMF will *"be free to claim (unlimited) damages against any volunteer where there are allegations of them behaving carelessly"*. It might help our understanding if you could explain your understanding of the specific scenarios that "gross negligence" or carelessness can apply to, in the context of Wikimedia volunteer activities, in plain English, that volunteers can then use as a reference to go back to, in the unlikely event of this becoming a reality. My apologies if I am misunderstanding your intended meanings here, though if I am having difficulty, I am certain others are too. Thanks --Fæ (talk) 00:21, 7 November 2013 (UTC)
> > > > I guess I'm not sure what the difference between "gross negligence" and "negligence" is - is there an accepted legal definition? Other than that, I personally am fine with it. --**Rschen7754** 00:36, 7 November 2013 (UTC)
> > >
> > > Good question Rschen. The difference between negligence and gross negligence will depend on the facts and the duty of care that someone exercises. Some helpful references are here on negligence and gross negligence. Geoffbrigham (talk) 01:10, 7 November 2013 (UTC)
> >
> > Thanks for the clarification Geoff. The English Wikipedia article you provide for a legal definition appears to show that the difference between negligence and gross negligence is a matter of debate and as clear as mud. I suggest if the WMF

wishes to have a legally enforceable policy and if anything goes wrong in the future it can be shown that volunteers accused of carelessness were clearly advised of the policy/pledge and its consequences in a way they could be judged to understand, then the WMF will have to define these terms in specific and appropriate ways that us volunteers do understand.
For example, as a Wikimedia OTRS volunteer the WMF has now stated that I have no legal protection or insurance, effectively if anything goes wrong then my house is at risk. If I agree to the pledge, does this mean that the WMF will help those that wish to sue me or that the WMF will sue me for damages themselves, say for carelessly pressing the send button on an email thread with personal or legal information in it, after putting in the wrong email address?
It would be really nice if at some point the WMF were to turn this around and put our minds to rest by offering liability insurance for unpaid volunteers that were taking on these functions for Wikimedia, in the same way employees were protected. This already happens in Chapters and other charities, it seems odd that the WMF is resisting this solution. --Fæ (talk) 09:11, 7 November 2013 (UTC)

> @Geoffbrigham: Having thought on this, I do wonder if adding "gross negligence" is opening up a can of worms, and maybe it should be left as "willful intent". "Willful intent" seems to be closer to the practice that I have heard from another staff member, as to their thoughts when they would pursue legal action (for extreme cases of someone revealing massive amounts of personal information). --**Rschen7754** 10:53, 15 November 2013 (UTC)
>
> > Hi Rschen7754 - Let's see what others say, but personally I'm fine with limiting statuary damages to acts of willful intent. Geoffbrigham (talk) 01:26, 16 November 2013 (UTC)
> >
> > > Hi Geoff, I am glad to see some movement on the odd word. A pity that the larger direct questions are seen to go unanswered. --Fæ (talk) 03:48, 16 November 2013 (UTC)

Bump. --**Rschen7754** 20:58, 3 December 2013 (UTC)

> Just a note that I've poked the lawyers for this thread. Jalexander--WMF 21:10, 3 December 2013 (UTC)
>
> > OK ... let's limit it to willful intent, given no other responses here. I will ask James to make the change. Geoffbrigham (talk) 21:36, 3 December 2013 (UTC)

Consideration of feedback given over the past week

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 19:13, 9 December 2013 (UTC)***

I would like to thank all of you who have provided very thoughtful feedback on this policy draft over the past week. Your suggestions and questions are much appreciated and have given us a lot to think about. We are internally discussing and brainstorming about many of the issues you have raised and I hope to provide more detailed responses and alternative suggestions over the next week. We may not get to everyone's comments as quickly as we hope to, but please be assured that we are reading and thinking about what each of you say in this discussion and will respond as best as we are able. Thank you again for taking the time to help shape and improve this policy draft. We sincerely hope that with the input we receive over the next few months, we will be able to craft a policy that reflects community values and adequately protects the privacy of both the community members who are in the valuable roles affected by this policy as well as the users whose nonpublic information they handle. Mpaulson (WMF) (talk) 17:24, 20 October 2013 (UTC)

Affected users who will resign if the policy is implemented in its current shape

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. It seems if we're going to have a list like this it should start anew given the large changes. Jalexander--WMF 19:19, 9 December 2013 (UTC)***

(this one (https://meta.wikimedia.org/w/index.php?title=Access_to_nonpublic_information_policy&oldid=6088605), where only non-central feedback was yet taken into consideration)

1. MF-W (steward, OTRS access) 22:04, 20 October 2013 (UTC)

> I haven't had time to read through your comments above quite yet, but it seems strange that nobody is editing the proposed policy to make it acceptable. It's a draft. Be bold! --MZMcBride (talk) 22:34, 20 October 2013 (UTC)
>
> > I think one of the main issues is that there is no specified/apparent reason for this change. It's a solution looking for a problem. It doesn't make sense to try and fix parts of it when the reason behind the entire thing is one of the biggest issues. Ajraddatz (Talk) 22:52, 20 October 2013 (UTC)
> >
> > > Do you agree with having wmf:access to nonpublic information policy? --MZMcBride (talk) 02:01, 21 October 2013 (UTC)
> > >
> > > > Your reply addresses nothing of what I said. I agreed to that policy when I identified to the foundation. You'll notice that I specify the need for change which is lacking, not the need for the policy in the first place. Ajraddatz (Talk) 02:11, 21 October 2013 (UTC)

Sorry, when you said "it's a solution looking for a problem," I thought you might mean having this policy was a solution looking for a problem, not updating it. I've attempted a better system of discussion below, though I understand that you feel a rewrite is entirely unnecessary. --MZMcBride (talk) 02:54, 21 October 2013 (UTC)

Ah. Sorry for my hostile response too, I assumed bad faith and thought you were trying to lead my logic to somewhere that I didn't want it to go. I've been studying Plato's works too much recently :/ Ajraddatz (Talk) 03:18, 21 October 2013 (UTC)

2. Trijnstel(talk) (steward, CU commons, CU meta, OTRS access) 22:17, 20 October 2013 (UTC) Unless some major changes are made ... otherwise I'm not sure I would stay.

   What kind of major changes? --MZMcBride (talk) 22:34, 20 October 2013 (UTC)

   I do not wish to re-identify so that the WMF can keep my ID. That change should be reverted (among others). Trijnstel(talk) 16:15, 21 October 2013 (UTC)

3. **Rschen7754** 22:28, 20 October 2013 (UTC) (Wikidata oversighter, OTRS access) Only because I have no money to give to the WMF if they sue me for an honest mistake.

   Noting that if the proposal as written passed as of this timestamp, I would be able to fulfill the requirements. --**Rschen7754** 10:47, 4 December 2013 (UTC)

4. Vituzzu (talk) (steward, OTRS access, meta checkuser) it should completely rewritten following a bottom-up process. 22:35, 20 October 2013 (UTC)
5. User:Nillerdk (OTRS access): I will not accept WMF to give away my ID to any third party, not even if required by US law. I will thus not give WMF in USA my personal informations under any circumstances. I *would* give personal informations to my local chapter, but I would only allow them to share my ID with third parties if required by national low in my country. Nillerdk (talk) 15:55, 21 October 2013 (UTC)
6. -**Barras talk** (steward, meta CU, meta OS, simpleWP OS, simpleWP CU, OTRS, CU-I admin if that matters, and while I'm on it probably just all rights straight away as protest, which includes several admin and crat rights along with my duties as GC for both groups, wikimedia/wikipedia and cvn) - As I'm not allowed by German law to re-identify under the condition, that WMF retains a copy of my ID card. See German laws §§14-20 PAuswG. I won't break German law to fulfill some weird rule here. -**Barras talk** 15:57, 21 October 2013 (UTC)
7. I probably would as well. I don't need these rights. So subjecting myself to such a potentially damaging situation is probably not in my future. -Djsasso (talk) 17:05, 21 October 2013 (UTC)
8. DaB. (talk) (OTRS-access, dewp-ml-admin, Toolserver-admin (until end of year) and I'm sure some more). The WMF is not able to protect such simple things as email-addresses or password-hashes, so I can not trust them with something as valuable as my passport. That the US is a 3th world-country in terms of Datenschutz is another problem. And finally I'm not allowed by German law to make a copy and give it to the WMF. --DaB. (talk) 19:21, 21 October 2013 (UTC)
9. Should the policy be adopted in its current state, I would have no choice but to let my identification lapse and hence be removed as steward and enwiki oversighter. While I truly enjoy the work we do here, and would love to keep doing it, the policy as it's worded is not acceptable, it's amateurish and it's stupid. It shows how little somebody at the WMF cares about our personal info, and does not make me sure enough that my information will be safe. I am more than willing to accept some compromise, but this is a scorched earth policy and it hurts me to see the WMF take this approach. We are volunteers, we built this projects or helped maintain them, we don't deserve to be treated like this. **Snowolf** How can I help? 16:57, 22 October 2013 (UTC)
10. The WMF can not be trusted bacause it is based in the US. It's that simple and I will resign my OTRS-access as soon as I am prompted to send a copy of my ID card. --McZusatz (talk) 14:53, 24 October 2013 (UTC)
11. --Natuur12 (talk) 21:10, 26 October 2013 (UTC) I will quite as an OTRS-voluntere if this policy becomes real.

Hi All. First, I would like to note that nothing in this policy draft is settled. The draft is just that...a draft. Anything contained within it is up for debate and suggestions. Second, we would really like to hear your thoughts on the discussion below about whether an identification policy is still needed. Thank you all in advance for your feedback. Mpaulson (WMF) (talk) 22:39, 24 October 2013 (UTC)

Volunteer developers

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 19:20, 9 December 2013 (UTC)***

There are some very weird ideas that a lot of people appear to hold about what/who the developers are. Some people think that we're all paid WMF staff. Others think that we're all system administrators. Those that think we're all system administrators probably think that we can all see nonpublic information. This document arguably makes that assumption or implication in a couple of places:

> "The following conditions are minimum requirements that all community members, including volunteer developers, must meet to qualify as a candidate."
> "All community members who are granted access to nonpublic information rights ("access rights"), except volunteer developers, are typically chosen by the community"

Volunteer developers are not automatically granted access to any nonpublic information. It's unclear to me whether or not this policy could cause any issues, but still... --Krenair (talk • contribs) 22:43, 20 October 2013 (UTC)

A fine point, Krenair. "Volunteer sysadmins and others with access to shared databases" might be more appropriate here. –SJ talk 19:40, 24 October 2013 (UTC)

Hi Krenair and SJ! This policy draft was meant to only cover volunteer developers who do have access to nonpublic information, not every volunteer developer. SJ, is there any risk with your suggested wording that it would inadvertently cover developers who only have access to shared databases that do not include nonpublic information? Mpaulson (WMF) (talk) 22:45, 24 October 2013 (UTC)

The language you use the first time it comes up in this document is good. –SJ talk 05:13, 25 October 2013 (UTC)

Policy should be rejected!

The following discussion is closed: ***Given how long this thread has been stale and the extensive changes since it was last active I'll archive it in a couple days unless reopened in order to clean up the page. Jalexander--WMF 19:22, 9 December 2013 (UTC)***

This is far beyond what is actually needed for the Wikimedia movement. I am feeling very uncomfortable if the WMF even thinks about this too far going proposal. After all the NSA/etc scandals this is what they come up with?? Sorry, absolutely no. In the whole text I see no reasonable explanation why extra requirements for identification are needed. A lot of bla bla but no actual reason why there is an actual need for. "*Because we believe that safeguarding the privacy of the Wikimedia community is an important Wikimedia value,*" -> if WMF is really thinking that, they wouldn't have proposed this policy that asks too much of giving up the privacy of volunteers. Romaine (talk) 01:12, 21 October 2013 (UTC)

Identity fraud is one of the most intrusive things people can experience. Identity fraud starts often with people knowing the birth date, as that information is often used for organisations to identify someone over the fone (etc). The WMF has no reason at all to keep copies/scans of an ID card. The government in the Netherlands forbids making copies/scans of IDs and also highly recommends not to disclose any information on the ID cards to unauthorized people. WMF is in the private sector and is not authorized to ask for this. Romaine (talk) 01:42, 29 October 2013 (UTC)

Hi Romaine. I just wanted to make sure you saw the more detailed reasoning laid out in the discussion below. I also wanted to make it clear that we are very open to alternate ideas about how community members with access rights identify to WMF and are interested in hearing your ideas. Mpaulson (WMF) (talk) 18:34, 31 October 2013 (UTC)

Attempt at a better evaluation of this draft

The following discussion is closed: ***Closing this whole section because it's all based on the old draft, including the quotes etc, and there hasn't been much response on it for a while partially because of that. Will archive in a couple days unless there is a reason to keep it open. Jalexander--WMF 20:14, 9 December 2013 (UTC)***

I'm going to try subsections and a cute template ({{talk page section}}) to evaluate each section of this proposed rewrite to wmf:Access to nonpublic data policy. I'm going to try to do this in a logical order. --MZMcBride (talk) 02:47, 21 October 2013 (UTC)

I am having difficulty of understanding the value of eating up volunteer time to create a detailed section by section or word by word review, when fundamental questions such as why this policy is needed, what the legal impact on unpaid volunteers is going to be and who will be given access to critical legal records of identity, have yet to be answered. The detailed text of the policy draft is likely to be significantly changed or have different assumptions underpinning it before these questions are resolved. Thanks --Fæ (talk) 13:06, 21 October 2013 (UTC)

The very first subsection covers the "why this policy is needed" needed question, doesn't it? Part of finding consensus is identifying areas of disagreement. We currently have a similar policy passed by the Board in 2007. Do you disagree with having this policy? If not, we should then discuss the proposed rewrite. If nobody agrees with any of the sections of the proposed rewrite, it'll be fairly trivial to reject the entire rewrite outright, right? --MZMcBride (talk) 13:17, 21 October 2013 (UTC)

No, it does not, this was raised earlier on this page and is still awaiting an answer. You cannot start a detailed document review, paragraph by paragraph, until the underpinning reasons for why the document exists and what impact enforcing it will have, is addressed. As to whether I disagree with this document or not may actually be irrelevant, the WMF are not legally bound to respect a community consensus here, and unless I missed it somewhere, I do not think they have stated anywhere that they shall respect a consensus as a management choice. --Fæ (talk) 13:40, 21 October 2013 (UTC)

+1. It certainly makes sense to write down comments section by section or piece by criticized piece, but this has already been done above by some users, see e.g. #Some food for thought by Snowolf. Comments are piling up on this page for about a week now, in which people protest against all sorts of sentences which they perceive as very objectionable in the draft. Meanwhile the Foundation hardly reacts. It is nice to read in #Consideration of feedback given over the past week that WMF discusses what we write and will at some time maybe react (hahaha), and that M. Paulson has even been answering here while being sick (which is, no doubt, sth. we can be grateful for), but afaik WMF has numerous people, also in its "Legal team", which surely is at fault for this draft, and it would be quite nice if they could at least devote the same time to discussing here as we volunteers do. Yesterday I was asked whether I hadn't commented at #Purpose 2 (a section whose content I agree with) yet - quite simply, I have already said what is expressed there in a different section on this page or on the checkuser-l list or on IRC (where also WMF staffers were present / able to read it). To sum up, I see all the same concerns being had by multiple people and being mentioned again and again, yet WMF is more or less silent. So I don't really have any motivation to contribute to such a systematical analysis of the proposal, when I see no reaction to comments anyway. --MF-W 14:35, 21 October 2013 (UTC)

> I don't think it's entirely fair to treat the legal team as if they're ignoring us because they don't have immediate answers. Remember, these are people with (for the most part) regular 9-5 daily jobs, who are trying to tick the boxes that they feel need to be ticked before they can present any proposal to us. When Michelle says they are discussing our feedback, I tend to think they're doing just that - discussing our feedback and trying to figure out how to integrate it with whatever it is they feel the policy needs to accomplish, per whatever WMF reasoning underlays that need (which, yes, it would be nice if they could get around to explaining that part to us). I don't think there's any doubt that they now understand just how vehemently people oppose the proposal as it's written (and there's no reason people can't keep sharing their opinions on the current proposal while we wait for a response), but these are lawyers, who need to get their wording bulletproof before they send it out into the world. If we're not willing to wait for them to have a coherent response, the other option is a handful of legal team members chaotically attempting to share what they personally think might happen once a new proposal is offered, followed by them having to backtrack once things change a little, and an end result much like some of the less pleasant software deployments we've had lately where no one knows exactly what "the response" is and everyone's reacting to something different. Rather than going down that rabbit hole, let's give Michelle, Geoff, and team a reasonable chance to respond in detail (in business-day time, not constant-wiki time) before we start assuming that they have no intention of working with us. Fluffernutter (talk) 15:31, 21 October 2013 (UTC)

Fæ: Re: "not legally bound to respect a community consensus here," you seem to be a bit confused about how policies like this are enacted. The Wikimedia Foundation legal team can certainly propose rewrites and can advocate for changes to this policy, however the Board decides. wmf:Access to nonpublic data policy is the current policy and nothing that the legal team does can undermine this. Whether the Board itself is strictly bound to follow community consensus is a tricky question. :-) In this particular case, we seem to have the bold (rewrite) and plenty of discussion, but little editing, which is worrying and against the typical BRD process. If there are problematic parts of this rewrite, let's figure out what those are and address them on-wiki. I think certain pieces of this rewrite are completely uncontroversial. Those pieces, at least, should be simple enough to resolve/approve before we get to the more difficult and contentious pieces. --MZMcBride (talk) 16:26, 21 October 2013 (UTC)

> Thanks for your concern that I might be confused. However I believe that your assertions that the WMF board of trustees (a partially elected body) overrules a Wikimedia community consensus, and that this WMF legal document can be changed by using the practices used on the English Wikipedia for writing encyclopaedia articles are not terribly helpful. --Fæ (talk) 19:22, 21 October 2013 (UTC)

> > If it helps, BRD is also documented locally. :-) This isn't a legal document and it's strange that you would suggest that it is. This document is a proposed rewrite to a standing Board-approved policy. Regarding supremacy, the Board is indisputably the ultimate arbiter (cf. wmf:Bylaws).
> > I have considerable experience in meta-matters and I'm trying to help move the discussion forward. Unfortunately, I'm not sure the same can be currently said of you. --MZMcBride (talk) 20:17, 21 October 2013 (UTC)

> > > I'm obviously unwelcome and you seem determined to make this discussion unpleasant and personal, so I'll not bother contributing further. Good luck with it. --Fæ (talk) 20:42, 21 October 2013 (UTC)

Policy itself

Status: In discussion

We currently have wmf:Access to nonpublic data policy, passed by the Board in 2007. Does anyone think Wikimedia should *not* have this policy any longer (i.e., the Board should get rid of this policy)? I believe there's general consensus to continue having this policy in some form, but before we go any further, we should make sure. :-) --MZMcBride (talk) 02:47, 21 October 2013 (UTC)

- It seems reasonable to have a policy. --MZMcBride (talk) 02:47, 21 October 2013 (UTC)
- So it does. –SJ talk 20:33, 24 October 2013 (UTC)
- There should be a policy about it and access to nonpublic data needs to be restricted, imo. -**Barras talk** 09:35, 26 October 2013 (UTC)

Title

Status: In discussion

Assuming you agree with having a policy of this nature, we can start at the top. There's a discrepancy between this page's title ("Access to nonpublic information policy") and the policy from 2007 ("Access to nonpublic *data* policy"). Should the title be changed? Should this page be moved? Thoughts? --MZMcBride (talk) 02:47, 21 October 2013 (UTC)

- The titles should be synchronized. I don't really care which is chosen. --MZMcBride (talk) 02:54, 21 October 2013 (UTC)
- Synchrony improves harmony. –SJ talk 20:33, 24 October 2013 (UTC)
- If this policy draft is adopted by the Board, there will only be one title (Access to Nonpublic Information Policy) because it would be replacing the current policy, so it will be synchronized. The reason why I changed it to "information" rather than "data" was to be consistent with the privacy policy draft which refers to things like "personal information" rather than "personal data" and I thought consistency between the two policy drafts would be helpful in that regard. Mpaulson (WMF) (talk) 22:45, 30 October 2013 (UTC)

User-friendly summary

Status: In discussion

There's a "user-friendly summary" at the top of the page:

Text of user-friendly summary [show]

Is it necessary to include a summary with this document? Does anyone agree or disagree with including this summary? (Please focus only on the summary's inclusion itself, the content itself will be discussed below.)

- I'm not sure a summary is needed here. --MZMcBride (talk) 02:48, 21 October 2013 (UTC)
- I find it useful but perhaps it could be briefer; I worry at the first list for instance, as it may be interpreted as comprehensive. --SJ talk 20:33, 24 October 2013 (UTC)
- We have generally received a lot of positive feedback about the user-friendly summaries. While I personally like reading through entire policies, I completely understand that most people are not like me in that regard. We hope that the user-friendly summary will alert people to the most important parts of the policy and allow them to easily find and read the details of the sections that are the important to them. We try to alert readers to the fact that the summary is not comprehensive with the disclaimer on top stating "Disclaimer: This summary is not a part of the Access to Nonpublic Information Policy and is not a legal document. It is simply a handy reference for understanding the full Access to Nonpublic Information Policy. Think of it as the user-friendly interface." Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

Purpose paragraph 1

Status: In discussion

Purpose paragraph 1 [show]

Does anyone agree or disagree with any part of this section?

- There's a semicolon splice ("content on the Sites;"). The final sentence doesn't make any sense. It says "Certain community members are entrusted with access to limited amounts of nonpublic information regarding others users, such as ...", but an example of limited nonpublic information isn't given. Instead, it tries to describe sockpuppeting to an outsider. This is a pretty strange sentence. --MZMcBride (talk) 02:51, 21 October 2013 (UTC)
- Thank you for pointing this out, MZ. As to your first concern, do you believe a comma would be more appropriate than a semicolon? As to your second concern, does this work better: To manage this immense task effectively, certain community members are entrusted with access to limited amounts of nonpublic information regarding other users. For example, a trusted community member who has "checkuser" rights could use those rights to investigate whether a single user is using multiple accounts in a manner inconsistent with Wikimedia policies. Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

Purpose paragraph 2

Status: In discussion

Purpose paragraph 2 [show]

Does anyone agree or disagree with any part of this section?

Scope paragraph 1

Status: In discussion

Scope paragraph 1 [show]

Does anyone agree or disagree with any part of this section?

- Does the "volunteer developer to access to nonpublic information" mean all Toolserver users? --MZMcBride (talk) 02:55, 21 October 2013 (UTC)
  - It's Labs now. --**Rschen7754** 18:53, 21 October 2013 (UTC)
    - Hi Rschen7754. Err, yes, I'm familiar with Wikimedia Labs. However, Toolserver users have access to the archive table and partial access to the user_properties and watchlist tables, among others. These database tables contain non-public information, which is why I asked the question I asked. --MZMcBride (talk) 20:19, 21 October 2013 (UTC)
- Does this include OTRS members? As we all know there is a major difference between stewards, checkusers & oversighters who have special access to the wikis and OTRS members who access correspondence that is separate from the wikis and where people know that their emails will be read by volunteers. I ask because it is worded *to view nonpublic information about other users*. OTRS members have access to nonpublic information but the term *users* usually refers to accounts on wikis which is possibly different from the clients send emails to the OTRS addresses. A significant part of the OTRS correspondence comes from people who never signed up as a user on any of our wikis. --AFBorchert (talk) 18:10, 22 October 2013 (UTC)

  This is worth specifying explicitly, as has been done in the past. –SJ talk 20:33, 24 October 2013 (UTC)
- MZ - This policy draft is intended to apply to Labs & Toolserver users who are granted access to nonpublic information. Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)
- AFBorchert - This policy draft currently only includes OTRS administrators, but we really would appreciate input from the community in the discussion above about whether it should also apply to OTRS agents. I agree that there is some ambiguity due to the term "users". I think if OTRS agents were to be included, we would change that to something along the lines of "view nonpublic information about other users or nonpublic information submitted through OTRS". I am open to alternate wording suggestions though. Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

Scope paragraph 2

Status: In discussion

Scope paragraph 2	[show]

Does anyone agree or disagree with any part of this section?

- "Election committee" is too unspecific. Nobody knows which one. --MF-W 14:24, 21 October 2013 (UTC)
  - Hmm, I agree. And broadly, how is the determination made as to whether this policy is applicable to a specific group? --MZMcBride (talk) 01:25, 22 October 2013 (UTC)
- Hm... are OTRS administrators included but not other OTRS members? I would suggest not to enumerate some samples but try to give a precise definition (see above) and/or try to enumerate all groups to which this applies now (with possible more coming). --AFBorchert (talk) 18:13, 22 October 2013 (UTC)

  I agree with the value in a precise definition. That also helps clarify why this policy exists in the first place. However a list of all affected groups should not be too long, and makes a useful supplement. –SJ talk 20:33, 24 October 2013 (UTC)
- The groups listed there are only meant to serve as examples. The more specific scope is defined earlier by what the individuals can do -- "Community members with access to any tool that permits them to view nonpublic information about other users (such as the CheckUser tool);Community members with the ability to access content or user information which has been removed from administrator view (such as the Suppression tool); and Volunteer developers with access to nonpublic information." I would not be opposed to listing more examples of groups (or even all of the groups we can think of that currently fall into these categories, but I'm hesitant to make an exclusive list because new groups could form, those groups could change names, and sometimes there may be certain people within a group that need to identify (because they have access to nonpublic info) while other people in that group do not (because they only have access to public info). Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

Requirements intro paragraph

Status: In discussion

Requirements paragraph 1	[show]

Does anyone agree or disagree with any part of this section?

- Please note that OTRS members and OTRS administrators are not chosen by the community of contributers. The question is if this point really needs to be elaborated here. I think it is best to remove this section. --AFBorchert (talk) 18:18, 22 October 2013 (UTC)
- I agree that "All... are typically chosen" may not be clear. The whole section could be reworded to focus on the requirements needed to get access to nonpublic data; rather than framing them as requirements for any particular selection process. –SJ talk 20:33, 24 October 2013 (UTC)
- That's a good point, AFBorchert. SJ - the reason why we included this section was to point out to more inexperienced users that the community members who have these access rights are trusted members of the community who have been vetted by the community. Do either of you have any suggestions as to how we could improve the wording in this section? Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

> How about this: *The following conditions are requirements that all community members should meet before being granted access to n.p.i.r. ("access rights"). These should also be considered requirements to be a candidate for any community-run selection process for a role that would convey such access rights.* –SJ talk 03:02, 3 November 2013 (UTC)

> > Hi SJ, I reworked the paragraph based on your suggestion. Thank you for your help! Mpaulson (WMF) (talk) 19:25, 9 December 2013 (UTC)

Requirements sub-point A

Status: In discussion

Requirements sub-point A [show]

Does anyone agree or disagree with any part of this section?

- This seems to unnecessarily disempower minors, considering how many of our extraordinarily competent, reliable, and talented administrators are smart high school students. If the concern is legal accountability, then a workaround involving a minor's legal guardian should be possible. If the concern is about practical accountability, then a signed statement may be equally effective (and most available remedies would be the same) for trusted community members who are not yet 18. Similar language was intentionally left as "may" instead of "must" in the previous version of the policy, and was not an oversight. –SJ talk 20:33, 24 October 2013 (UTC)
- I'm reposting my response from the discussion below just in case people missed it there: The switch from "may" to "must" was meant to get rid of the ambiguity. My understanding was, in practice, that all community members with access to nonpublic information (except OTRS agents) were required to be 18 years old and the age of majority for their jurisdiction. The reason for this in the current policy, as I understand, was to ensure personal accountability. From a legal standpoint, it is easier to hold an individual personally accountable if they are the age of majority. I saw no reason to leave the ambiguity of "may" in this draft policy if the purpose was to actually have an age minimum. That said, the age minimum (like anything in this policy draft) is not set in stone. It can be raised, lowered, or done away with all together. I'd like to hear what other community members think about the age minimum. Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

Requirements sub-point B

Status: In discussion

Requirements sub-point B [show]

Does anyone agree or disagree with any part of this section?

- This sounds as if the original document of identification has to be passed to the WMF. But this is probably not meant. I understand that the WMF needs some sort of proof of identification but I think it is best to move this to a separate point how this can be done. This section unnecessarily asks for identification documents (or possibly scans thereof) to be handed over to the WMF without considering alternative approaches. As pointed out above this is not just uncomfortable for many functionaries but also in conflict with local legislations. I would like to see here more openness towards solutions that provide the necessary proof of identification but which are more consistent with the preferences and the legal environments of the functionaries. It should be possible, for example, to handle this through the local chapters and possibly third parties. (For example, there exist identification services like Postident in Germany which could be utilized through the WMDE local chapter.) --AFBorchert (talk) 19:34, 22 October 2013 (UTC)
- I agree with AFB: I would strongly approve of any mechanism that does not require community members to send identifying documents to servers in a different country. –SJ talk 20:33, 24 October 2013 (UTC)
- Hi AFBorchert and SJ. This section was indeed meant to require a copy or scan of an identification document to be sent to WMF, not the original document. My apologies for the confusion. That said, we are very open to alternate forms of identification submission and retention and are soliciting suggestions from the community. You may want to see my response in the discussion below. I'd love to hear your ideas. Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

Requirements sub-point C

Status: In discussion

Requirements sub-point C [show]

Does anyone agree or disagree with any part of this section?

- This helps clarify what is being committed to. –SJ talk 20:42, 24 October 2013 (UTC)

Requirements sub-point D part I

Status: In discussion

Requirements sub-point D [show]

Does anyone agree or disagree with any part of this section?

- This requirement has a giant loophole. Why bothering about locked cabinets and password protection when arbitrary third parties with a non-disclosure agreement and unknown policies have unrestricted access to it? Leaks happen. And the best protection against leaks is to minimalize the amount of sensitive materials you collect. Hence, I do not understand why *physical copies of submitted materials* are required. A name and a postal address should be sufficient. (This is at least sufficient in Germany, see de:Ladungsfähige Anschrift.) --AFBorchert (talk) 19:47, 22 October 2013 (UTC)
- A few people have noted that (A) is not clear here. I do not understand the value of keeping other original documents around -- not trusting the initial authority used to verify them and needing to reverify? -- and would appreciate further explanation. There are valid reasons for people, particularly those who live outside of the US, to be wary of having personal documents permanently stored on servers in the US. The reasons for having access to originals that I can think of might be satisfied by either re-requesting them as needed or by having a document-escrow of the person's choice. –SJ talk 20:33, 24 October 2013 (UTC)
- Hi AFBorchert and SJ. As mentioned in the discussion below, we are very open to different forms of submission and retention and would like to hear your suggestions. Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

Requirements sub-point D part II

Status: In discussion

Requirements sub-point D part II [show]

Does anyone agree or disagree with any part of this section?

- In my opinion, this section should be killed. Retention (if any) should only happen during active use of the tools. A three-year period after seems unnecessary. --MZMcBride (talk) 03:07, 21 October 2013 (UTC)
- As pointed out above, it should be sufficient to keep the verified name and postal address of someone with access to nonpublic information. This would also be sufficient in the example you give. There is no need to keep copies of government-issued identifications. --AFBorchert (talk) 19:53, 22 October 2013 (UTC)
- This section seems too broad. An exception should be made for someone whose use of nonpublic information is being investigated (which may be the reason for loss of rights). But otherwise, there should be little need to retain most information. I can see keeping a very-limited historical record to avoid gaming the process: for instance, to keep a single person from identifying many times linked to different on-wiki identities. But some submitted materials (such as copies of formal IDs) could be deleted promptly; others (such as address/contact information) could be deleted soon after rights are given up. –SJ talk 20:33, 24 October 2013 (UTC)
- Thank you for your feedback on the retention period issue, MZ, AFBorchert, and SJ. I'd also like to point out that a related discussion is occurring above in case you want to see what others are saying. I'd also be curious about your thoughts on a 6 month following retirement of access rights retention period mentioned there. Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)
- No opinion yet on the general idea, but I'd note that "If a community member ceases to have access rights, he or she should notify the Stewards" doesn't really make much sense. The Stewards are the ones who revoke access like this in the first place, so why would they need to be notified? — **PinkAmpers&** (*je vous invite à me parler*) 04:16, 15 November 2013 (UTC)
  - Hello @PinkAmpersand: as an update, that section has now been removed (https://meta.wikimedia.org/w/index.php?title=Access_to_nonpublic_information_policy&diff=6451564&oldid=6222708) from the policy now. Thanks, 22:32, 3 December 2013 (UTC)

Submitting new materials

Status: In discussion

Submitting new materials [show]

Does anyone agree or disagree with any part of this section?

- Again, this section implies that there is a need to keep copies of submitted materials. --AFBorchert (talk) 19:55, 22 October 2013 (UTC)
- Hi MZ! I wanted to repost what I just said in response to Risker in another portion of this discussion concerning the retention period in case people commenting here miss it up there.

> The reason why we had decided on 3 years is that when discussing potential periods for retention with the Ombudsman Commission, it seemed possible for an investigation concerning the actions of a community member with these kinds of access rights to still be ongoing 2 years after the community member in question had resigned their rights. This could be the case in a particularly complex investigation or one that did not come to the attention of WMF or the Ombudsman Commission until after the community member resigned their rights. That said, I understand that 3 years can be perceived as a long time and if the community believes that investigations of these kinds are all but rarely resolved in a shorter period of time than 3 years, I'm certainly open to hearing what they believe is a more reasonable length of time. Mpaulson (WMF) (talk) 21:40, 22 October 2013 (UTC)

> > Probably, if we look to European standards, a reasonable time is ≤\0. --Nemo 08:32, 28 October 2013 (UTC)

Submission methods

Status: In discussion

Submission methods [show]

Does anyone agree or disagree with any part of this section?

- Again, this is unnecessary as there exist alternative approaches to provide a proof of identity. --AFBorchert (talk) 19:58, 22 October 2013 (UTC)

Submission timeline

Status: In discussion

Submission timeline [show]

Does anyone agree or disagree with any part of this section?

- This paragraph fails to outline how the users with access rights will be notified and/or warned. And I think that some time should be given to develop alternative techniques to provide a proof of identity. (This does not need to be covered by this policy. There could be a process that approves alternative approaches.) --AFBorchert (talk) 20:05, 22 October 2013 (UTC)
- As I've mentioned above, we are open to alternative forms of proof of identity. However, I want to assure you that should any requirement submit identification documents or submit identifying information be adopted here, we will do whatever we can to notify any affected users about the new policy and what needs to be done. Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

Use and disclosure intro paragraph

Status: In discussion

Use and disclosure intro paragraph [show]

Does anyone agree or disagree with any part of this section?

- This section helps clarify what is at stake. –SJ talk 20:42, 24 October 2013 (UTC)

Use and disclosure sub-point A

Status: In discussion

Use and disclosure sub-point A [show]

Does anyone agree or disagree with any part of this section?

- This description does not match the activities of OTRS members. They are not always strictly in the business of preventing, stopping, and minimizing damage to the sites and its users. --AFBorchert (talk) 20:09, 22 October 2013 (UTC)
- Leeway for good judgement would be helpful here and in subpoint B. –SJ talk 20:33, 24 October 2013 (UTC)
- AFBorchert - As mentioned above, the decision as to whether OTRS agents should be included in this policy is still being discussed. However, I would be very interested in your suggestions as to how we could edit this section to include a description of what OTRS does. Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)
- SJ - Could you clarify what you mean by providing leeway for good judgment? Do you have any suggested wording that would illustrate what you mean? Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

  A suggestion for AFB's point: *...solely for activities that protect and help the Sites and their users. Community members with access rights may only use those rights and the subsequent information they access under the policies that govern the tools they used...*
  I'm not sure of the right legal phrasing for good judgement. Perhaps "activities that, in their judgement, protect and help"? I'm not sure how important this is here. But it's usually not clear whether an action actually will have those effects; and the whole point of choosing people for their sensibility is that we are placing that trust in them. So it seems reasonable to me to call that out here. –SJ talk 06:08, 3 November 2013 (UTC)

    Hi SJ, I made some changes based on your suggestion, which hopefully addresses your point. Thank you for the suggestion! Mpaulson (WMF) (talk) 19:37, 9 December 2013 (UTC)

Use and disclosure sub-point B

Status: In discussion

Use and disclosure sub-point B [show]

Does anyone agree or disagree with any part of this section?

- In the current practice of CU cases, some nonpublic information possibly gets public like for example the information which accounts are related. When a CU case includes anonymous accounts identified by their IP addresses, this can be quite revealing. I do not see how this practice is covered by this section. Likewise, it is common practice to publish selected nonpublic information from OTRS correspondence. For example, in a permission case, OTRS members publish the before non-public fact that a copyright owner releases some media or text under a free license. What needs to be exercised is good judgement. Checkusers have a great responsibility when they publish their report of the CU results and likewise OTRS members must carefully judge what can be made public. This section as it stands does not address this. --AFBorchert (talk) 20:22, 22 October 2013 (UTC)
- See above. –SJ talk
- That is an excellent point, AFBorchert. Do you have any suggestions as to how to best address the OTRS scenario that will still protect against the public release of sensitive information often included in OTRS correspondence? As to the CU case, that example was brought up by someone else and

we are trying to figure out a way to address that situation directly in the policy. Any suggestions you have would be greatly appreciated! Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

> Hi AFBorchert. Just wanted to circle back on this and let you know that we added an additional disclosure scenario to this section in the new draft that hopefully addresses this issue. Thank you for your help! Mpaulson (WMF) (talk) 19:43, 9 December 2013 (UTC)

Penultimate paragraph

Status: In discussion

Penultimate paragraph [show]

Does anyone agree or disagree with any part of this section?

- This seems reasonable. --MZMcBride (talk) 03:10, 21 October 2013 (UTC)
- +1 –SJ talk 20:33, 24 October 2013 (UTC)

Final paragraph

Status: In discussion

Final paragraph [show]

Does anyone agree or disagree with any part of this section?

- There are two different e-mail addresses? legal@ and check-disclosure@? This seems confusing. --MZMcBride (talk) 03:09, 21 October 2013 (UTC)
- Actually there's a different situation which should be taken in consideration: if a checkuser living in, for example, Spain, is asked by local authorities to *quickly* disclose and IP of an user posting onwiki its intention to commit suicide. I know this kind of situation has been already managed, but WMF must take into account it re-writing a policy which seems to presume checkusers are criminals by nature. --Vituzzu (talk) 11:54, 21 October 2013 (UTC)
- MZ - legal@ is where anyone who wants to request user information from WMF should send those requests. If a community member receives such a request that falls out of the purview of their role or if they are simply uncomfortable responding to such a request, they should pass those requests onto WMF by sending it to legal@. In contrast, check-disclosure@ is where you should alert WMF that you have disclosed user information to a third party. Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)
- Vituzzu - that scenario should be covered by "In the course of keeping the Sites and its users safe, community members with access rights must sometimes disclose nonpublic information to third parties. Disclosures of nonpublic information may be made to:...law enforcement in cases where there is an immediate and credible threat to life or limb;" Mpaulson (WMF) (talk) 00:11, 31 October 2013 (UTC)

Notifications

The following discussion is closed: ***closing this since it's been more then a month without response. I think we've reached out to all groups that need it (some a couple times) but if there are others who need it please let me know, I'm happy to try and reach out to others. Will archive in a couple days unless reopened. Jalexander--WMF 20:35, 9 December 2013 (UTC)***

As I already asked on wikimedia-l without answer from WMF: were all the checkusers, OTRS volunteers etc. specifically notified about this draft and discussion which matters them directly, on their email addresses or talk pages? It would be better if the WMF did so, as only WMF knows why we're having this discussion, but time is running: if they don't plan to, can someone use global message delivery to notify them? Objections? --Nemo 06:52, 24 October 2013 (UTC)

> I know all CU/OS/stewards received an email, but I get the feeling that some groups got left out, especially as there is no concrete definition of who is affected by this. --**Rschen7754** 07:00, 24 October 2013 (UTC)
> (e/c)All checkusers, oversighters and stewards were notified by email. I mentioned this above somewhere as well after being asked about it. I know that the enWP ACC tool users (who identify because of their IP access on the tool) were also notified. I have not notified OTRS agents yet because we had not determined exactly how they would be affected, the policy as written did not envision including them (similar to the current policy which puts them into a special category) and the privacy policy was written with that assumption as well (lack of privacy when you email) though I know that it has come up and we would probably need to put an exception into this one similar to the current one. That wasn't added when it was brought up earlier because of the ongoing discussions, my guess at the moment (assuming we continue to check IDs) is that we will have a separate discussion to figure out OTRS which they will obviously have to be notified about. When it came to that I'd probably work with the OTRS admins because I know they have sent mass emails to all agents before. Jalexander--WMF 07:07, 24 October 2013 (UTC)
>
> > Actually I think that all users should be informed about this major change, no matter what user groups they belong to. Of course it is more important for the users who are directly affected by this, but there might be people out there who plan on becoming OTRS agents, checkusers or oversighters on their projects and don't know that this policy may be changed in future. There might be people who want to run for the next steward elections, not knowing about this. Not only users with access to nonpublic information should be informed, but also the people whose nonpublic information we are talking about. I'd like to see some notification about this for all users rather soon. It's not fair to inform only a subset of people instead of all! -**Barras talk** 08:10, 24 October 2013 (UTC)

OTRS users sure weren't - David Gerard (talk) 13:46, 24 October 2013 (UTC)

As Rschen7754 notes, some possibly affected user groups were likely not notified because there's ongoing ambiguity about what the scope of this proposed rewrite is. I believe the current interpretation is that this proposed rewrite would only apply to OTRS administrators, not OTRS users. But at this rate, I think the entire rewrite will be scrapped. --MZMcBride (talk) 14:20, 24 October 2013 (UTC)

@Risker: Would functionaries-en subscribers be required to identify, even though many of them are ex-arbs who no longer hold CU/OS? --**Rschen7754** 18:55, 24 October 2013 (UTC)

If it's about notifications I know I emailed them when we sent out the CU/OS notifications (to make sure they got it). Whether they would need to re identify even if they no longer hold CU/OS to remain on the list is an interesting question I'm not sure had been thought about... Jalexander--WMF 00:09, 25 October 2013 (UTC)

It applies to me and just a couple others (although I guess I might also have to identify for OTRS). It's not like a bunch of folks at the WMF don't already know who I am, so I don't have any problem with identifying again in principle, but it would be a pain... NW (*Talk*) 22:29, 25 October 2013 (UTC)

yeah, as usual on these types of edge cases it would have to be a bit of a case by case analysis (since circumstances change etc) but talking with Philippe a superficial look at functionaries-en says that we would likely not force non CU/OS users on the list to identify. Jalexander--WMF 22:41, 25 October 2013 (UTC)

- Note: I'm reaching out to the OTRS admins now to alert all OTRS users of this discussion and the discussion above about if we should include them in the policy. Jalexander--WMF 21:42, 25 October 2013 (UTC)
- Why are not **all** users informed about this discussion? It's good that the people with access to nonpublic information are informed, but I fail to see a reason why the people whose information we are talking about are not informed. I think that everyone should have their say here, and I think everyone deserves it to be informed. Of course the CUs, stewards etc etc are more affected by this, but trying to look at this from outside, as a normal user, I'd like to be informed about that change. There might be users who want to know who deals with their private/nonpublic information and what the rules about this are like. Even thought that is an open discussion and everyone may find this place themselves, I doubt that all users are actively searching for such stuff. Looking at the page, mostly/only people who were informed take part in that discussion. Other people may also have good ideas and wish to comment. I'm really disappointed about the information flow about this. -**Barras talk** 12:53, 26 October 2013 (UTC)

The idea was that we were doing this as part of the privacy policy discussion because they are very tightly linked (and changes in here may require changes in the privacy policy). We had a blog post and mailing list announcement (both of which had a whole paragraph talking about this policy) and ran banners both to logged in and anonymous for the privacy policy with links to the blog post in the introduction and links to this policy and discussion on that feedback page. Given that the privacy policy was the center piece of the discussion and we were talking about this in that context it did not seem to make sense to have separate banners for this policy (especially since we were sharing with Wiki Loves Monuments and Fundraising, both of which were pushing for us to lose less space already.. which we were telling them no on). If people think that we should do some more out reach I'm certainly open to it, this is also why we had such a long (and somewhat open ended) feedback period to make sure we could try and get as wide a net of feedback as well. I've always somewhat intended to throw the banners on for another week at one or two different periods over the course of the 4-5 months we are discussing. Jalexander--WMF 10:32, 27 October 2013 (UTC)

Agreed, I work in Account Creation, and I see personal info with every request. Anyone who works with personal information should be notified of this discussion. --Sue Rangell (talk) 19:52, 2 November 2013 (UTC)

feedback from otrs agent

The following discussion is closed: ***Closing given how long it has been since the last edits and the large changes on the draft since then. Will archive in a couple days unless reopened. Jalexander--WMF 20:51, 9 December 2013 (UTC)***

As for I, I have totally given up with the idea of preservation of confidential data when the US are somehow involved (if the NSA is already involved in recording German president phone conversations or French diplomatic department communications, who are we to hope that our every steps can be private anyway ?).

My trust in WMF ability to provide security to our private information also dramatically dropped with the password leak a couple of months ago.

Hi Anthere. I completely understand your concerns here. The actions of the NSA have shocked and upset us all. As for the hashed password leak, that was a very unfortunate incident and one we are working to ensure never happens again. Mpaulson (WMF) (talk) 21:40, 30 October 2013 (UTC)

So what are the risks left ? I see mostly three main ones

disagree with preservation of digital version of id papers

1) that a digital version of my passport get in the hands of scammers. We know some of the risks associated to this, one of which being identity theft. Collection of a bunch of private data (name, email, phone number, postal address...) is one thing. Preservation of official identity paper is another.
I think that's a non-acceptable risk.

> We are open to ideas about how the identification documents are stored. Are you against any kind of digital submission or retention of documents or are there certain security measures like encryption that would make this option more palatable to you? If you do not think any digital submission or retention is safe enough, would mailing you identification documents and retaining them in a safe be a sufficient alternative? You may want to look at a related discussion below regarding whether storing identifying information rather than copies of the identification documents themselves would be sufficient and leave some thoughts there as well. Mpaulson (WMF) (talk) 21:40, 30 October 2013 (UTC)
>
> > Answered below. Anthere (talk)

disagree with disclosure of agent private information to community members not bound to the non public information policy

2) that WMF disclose private information about us (OTRS member for example) volunteers to other volunteers, who may not even be identified in the least (as in "arbitration committee members").
Main risk associated imho would go from mild online bullying to severe irl mishandling. I have very acute memory of this sick person sending me emails threatening my life and the life of my own kids when I was Chair of WMF. I was happy he was in the USA and me in France. I was not happy he knew of my postal address. And I was scared when I met him at the WMF doors irl.
Disclosing private information about us to a lawyer or a policeman is one thing. Disclosing private information about us to an "unknown" wikimedia member not bound by similar rules related to private data is unacceptable.

> I'm a little confused about this comment. WMF would not disclose information from the submitted identification documents to other volunteers. Under the applicable clause in this draft, "The Wikimedia Foundation will not share submitted materials with third parties, unless such disclosure is (A) permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department; (B) required by law; (C) needed to protect against immediate threat to life or limb; or (D) needed to protect the rights, property, or safety of the Wikimedia Foundation, its employees, or contractors." I assume you are referring to the text in the subsection following stating: "Sometimes, the Wikimedia Foundation or a user community committee will need to contact a community member who formerly had access rights about his or her usage of those rights. For example, the Arbitration Committee may need to complete an ongoing case they are examining or the Wikimedia Foundation may need to notify you of receipt of a legal document involving that community member." This section was meant to explain the reasons for retention of your identification information. WMF would not give your identification information to other volunteers in this situation. We would contact you using the information you submitted to us to let you know that ArbCom needs to get ahold of you regarding an ongoing case. Would clarifying that in the policy draft help? (And obviously let me know if I'm misunderstanding your concern here and therefore inadequately addressing it.) Mpaulson (WMF) (talk) 21:40, 30 October 2013 (UTC)
> Yes, if this is what you have in mind, I think a clarification of the text would be best. I read that our data may be given to arbcom members for example. Anthere (talk)

ask for mandatorily notification of non public information disclosure about agent from WMF to concerned agent

3) last, that WMF disclose private information about us without having the obligation to inform us it did so.
The draft proposes that *The Wikimedia Foundation will not share submitted materials with third parties, unless such disclosure is (A) permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department; (B) required by law; (C) needed to protect against immediate threat to life or limb; or (D) needed to protect the rights, property, or safety of the Wikimedia Foundation, its employees, or contractors.*
This is vague enough that it may happen that our private data is disclosed to about whoever (who will access our private data thanks to this "permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department" ???), possibly without us knowing.
Consequences may be various (being citing in a legal case without even knowing; having personal information disclosed to spammers or scammers; being sued by an "unhappy customer" after we failed to fix his case on otrs etc.)
A good part of benefit of this agreement would be that covered person better feel accountable.
I think a fitting balance would be that WMF agree to mandatorily inform ANY covered person WHEN and to WHOM his/her information has been disclosed. Accountability both way. Naturally, WMF would also engage itself to inform us when it fucked up (as it did well with the password leak) Anthere (talk)

> I agree completely. In fact, the protections that you speak of are currently in the forthcoming "Requests for User Information Procedures and Guidelines". We are working with the EFF to finalize it and will be releasing it publicly soon. The very purpose of these guidelines is to let anyone -- litigants, governments, police authorities -- who wants user information from us know what standards they need to meet before we are willing to release any user information. The guidelines also specify that our default position is to inform the affected user (if we have contact information for them) that such a request has been made and by whom so that the user can use any legal remedies available to them to stop the release of their information. Mpaulson (WMF) (talk) 21:40, 30 October 2013 (UTC)
>
> > Good (great); Waiting for the forthcoming RUIPG then. Anthere (talk)

Comments

Good points and some scary but true illustrations. I would like to add that I would be a lot more comfortable if I knew that were a scan of my passport to ever be leaked on the internet and I was then subject to identity theft, was then forever internationally blacklisted for credit, falsely thought to be a terrorist by the NSA and could never do business in the USA, or suffered other damages, that the WMF (or their agent with authority to hold the records) had excellent data protection insurance that I could then easily claim something in the order of $2,000,000 compensation to make me feel better about my damage and distress caused by my unpaid volunteer work that happened to require identification. Thanks --Fæ (talk) 14:16, 26 October 2013 (UTC)

Agreed. Anthere (talk)

WMF has secured insurance coverage as deemed appropriate by our Finance department.Mpaulson (WMF) (talk)

Sounds good, as the volunteers that are protected by this insurance, can we look at it please? I would like to know how much I am covered for if someone emailing OTRS tries to take me to court for whatever reason and requires the WMF to reveal my legal identity. Thanks --Fæ (talk) 22:46, 30 October 2013 (UTC)

After Geoff's clarification in a previous section, I now know that there is no "data protection insurance" for volunteers, nor does the WMF have any plans to fix this lack of insurance cover. In this context I feel the answer given that "WMF has secured insurance coverage as deemed appropriate" when the fact is there is no such insurance, was more political spin than a real answer and considering the intention of my comment was extremely clear and illustrated with examples, I feel this was misleading. In practice this means that to get any damages/compensation after suffering identity theft or fraud, a volunteer would probably have to sue the WMF for mishandling their personal data so that in turn the WMF could claim this against insurance that protects them but not the volunteers. I hope that answers to other questions on this page by the WMF have been more straight-forward. --Fæ (talk) 10:43, 15 November 2013 (UTC)

- Thank you for posting these comments here Anthere, I was about to copy them from the mailing list and noticed you already had. Would you mind if I (or you) either adjusted the header or split off #3? I want to make sure that the specific comment on notification gets attention (the other pieces are important as well but I think they are generally covered under other sections which I know are already on the list for discussion and consideration). Jalexander--WMF 06:12, 27 October 2013 (UTC)
  - is that okay this way ? If not clear enough, do not hesitate to edit my part. Anthere (talk)

Illegal

The following discussion is closed: ***Closing given how long it has been since the last edits and the large changes (including removal of physical ID) on the draft since then. Will archive in a couple days unless reopened. Jalexander--WMF 20:52, 9 December 2013 (UTC)***

In the Netherlands it is illegal to request a copy or scan of a passport or ID card. In the private sector only banks and employers are an exception in that by law.[1] (http://www.telegraaf.nl/binnenland/20791004/__Kopietje_paspoort_verboden__.html)[2] (http://www.cbpweb.nl/downloads_rs/rs_kopie-identiteitsbewijs.pdf) In all other cases it is forbidden to make copies or scans of it. By law we must report any organisation that still requests it, as it is illegal. Romaine (talk) 21:22, 26 October 2013 (UTC)

On the tangential subject of national variations—a slight wrinkle for UK citizens is that we are not required by the state to have any standard ID, and there is no standard identity card even if I wanted one. My passport happens to be the only photo ID I possess, so when that expires next month, I will not have any form of official photo ID to present to anyone. As it happens I have an old form of driving licence, no photo, again UK government does not require me to update to the photo-ID driving licence which was introduced in 1998, so it is just a big piece of paper; it confuses the hell out of people when I try and hire a car. --Fæ (talk) 21:51, 26 October 2013 (UTC)
Hi Romaine, can you clarify the relevancy of the point you make above? Since the WMF is not located in the Netherlands, it's unclear to me. **Nathan** T 14:28, 27 October 2013 (UTC)

Aren't WMF's esams and knams servers near Amsterdam, The Netherlands? --**Krenair** (talk • contribs) 14:38, 27 October 2013 (UTC)

Nathan, the actions of the WMF in enforcing policies for Wikimedia volunteers should not just be literally "legal", but being seen as a global charity ought to be lawful. In this case though the WMF may argue the case that it would not be *technically* breaking the law in the Netherlands, the common sense rules for NL businesses and the public still apply. I suggest taking a look at the documents that Romaine has linked to, they seems to support the exact same concerns that have been raised by other volunteers on this talk page. --Fæ (talk) 16:59, 27 October 2013 (UTC)

Romaine, is it also illegal to *provide* such copies? --Nemo 20:13, 27 October 2013 (UTC)

Romaine, how does a business that needs to identify you in the normal course usually do it in NL then? (For instance, if you rent some expensive bit of equipment, the lender would normally need to have some way to keep you accountable).
— Coren (talk) / (en-wiki) 14:04, 28 October 2013 (UTC)

> They probably look at the ID card and simply note down the needed data (address, name, date of birth) or put it into their data bank without keeping a scan/copy of the ID card. We've similar laws in Germany. The ID card my be used to verify the data/person, but it is not allowed to retain copies of it. See German laws §§14-20 PAuswG. -**Barras talk** 16:06, 28 October 2013 (UTC)
>
> > Just as Barras says, showing the ID card is sufficient (in most cases noting down the info from the card isn't needed). Scanning/copying is only allowed in case of a juridical base: a legal obligation. In other cases it is forbidden to copy/scan. The Dutch government is keen on preventing identity fraud and other forms of fraud with identification. Romaine (talk) 01:35, 29 October 2013 (UTC)
> >
> > > If this is confirmed, it's obvious the policy will have to include at the very least an exception for the Netherlands (and any other country forbidding to make copies of identity documents): the WMF can't solicit, let alone force, anyone to commit illegal activities. --Nemo 06:52, 29 October 2013 (UTC)
> > >
> > > > Can they do it with people in other countries though? I would've thought that since they have servers in the Netherlands, Dutch law applies to them. --**Krenair** (talk • contribs) 16:12, 29 October 2013 (UTC)
> > > >
> > > > > IMO it would better to establish a standard that works for everyone, rather than have some people with copies of IDs and others with just stored information. Ajraddatz (Talk) 02:07, 30 October 2013 (UTC)

Hi All! Thank you for sharing your concerns here. We are certainly open to ideas on how identification should be handled. Accordingly, I'd like to get some thoughts on a few things below (and please feel respond in-line for the sake of clarity.) Mpaulson (WMF) (talk) 19:02, 30 October 2013 (UTC)

> First, does anyone have alternate links to the information Romaine provided? I seem to only get error messages when I try them. Mpaulson (WMF) (talk) 19:02, 30 October 2013 (UTC)
>
> 1. rs_kopie-identiteitsbewijs.pdf on web.archive (http://web.archive.org/web/*/www.cbpweb.nl/downloads_rs/rs_kopie-identiteitsbewijs.pdf)
> 2. Telegraaf article on web.archive (http://web.archive.org/web/20131101064727/http://www.telegraaf.nl/binnenland/20791004/__Kopietje_paspoort_verboden__.html)
>
> --Fæ (talk) 06:53, 1 November 2013 (UTC)

> Second, given the restrictions on providing copies of identification documents to third parties in some countries and the lack of requirements to have any identification documents in other countries, what do you all think would be an acceptable method of checking identification? Would simply submitting your real name and current email address suffice? Should a mailing address or telephone number be required? Are there alternate ways that one can prove their identity other than submission of a government-issued identification document? Should everyone be required to submit their information the same way or should there be different options for people to choose from? If the latter, how do we ensure that the different options are of roughly equivalent credibility? Mpaulson (WMF) (talk) 19:02, 30 October 2013 (UTC)

> Third, should the information submitted (whether it be a copy of an identification document or simple submission of a name and email address) be verified in some fashion? If so, how? If not, why not? And if so, should it be periodically re-verified and how often? Mpaulson (WMF) (talk) 19:02, 30 October 2013 (UTC)
>
> > Firstly, a simple method to verify a postal address is to send a letter to it with some token that allows to confirm that it was successfully delivered and received by the intended recipient. This approach is simple and does not break any laws. It just takes some time.
> > Secondly, I do not see a problem if multiple options are provided where people can freely chose from. You do not need an equivalent amount of credibility, just some minimal threshold which is to be met. No method of identification is safe against falsification. But please remember that you are requiring identification from people who have already trust from the community.
> > Thirdly, it should be sufficient to simply ask all volunteers who work under this policy to update their address etc. if it changes. --AFBorchert (talk) 19:35, 30 October 2013 (UTC)
> >
> > > And obvious cases should please be handled as obvious cases. Some prefer pseudonyms but many of us work already with their real name all the time (like me). You will find my full name on all my major wiki user pages, you find a backlink to Wikimedia Commons at my private website (http://www.andreas-borchert.de/), whose domain is owned by me (there are public records with my name and address at DENIC), and whose IP address (currently 217.10.8.60) when submitted to RIPE delivers multiple contact records including AFB13-RIPE (https://apps.db.ripe.net/search/query.html?searchtext=AFB13-RIPE&searchSubmit=search) which delivers my full address including phone number. You need of course a general solution for the identification problem. But I would appreciate it if obvious cases (like mine) need no further bureaucratic procedures. --AFBorchert (talk) 19:49, 30 October 2013 (UTC)
> > >
> > > > Thank you for your thoughts and suggestions, AFBorchert.
> > > >
> > > > > Postcards to verify address have been mentioned multiple times. Another option, to verify at least name and potentially more, is a symbolic payment: PayPal uses it, it's the only legal identification method for bank accounts "portability" in Italy, etc. A 0,01 € bank transfer to your SEPA bank account will be an extremely easy and cheap option for many in EU (you could also pay it back, I hope WMF doesn't pay fees for such SEPA payments). It wouldn't work for everyone, of course; just adding to the list of ideas. --Nemo 20:09, 31 October 2013 (UTC)

> I would like to add into the mix that any trusted user that is, or has been in the past, a trustee or director of a legally incorporated Wikimedia Chapter or Thematic Organization has public records of their directorship available as a public record. I believe that in most countries this means that there is a record of their directorship that is fairly easy to link to on the internet. Directorships have been verified against legal IDs (which acts as protection against money laundering) and have been accepted by the WMF under the Chapters Agreement. Personally, I don't mind sending the WMF a link to my online directorship records as they are already a public record; this avoids the bizarre discussion we will have when the WMF asks me for valid photo ID and I say I don't have any, as it is not required in the UK. --Fæ (talk) 07:04, 1 November 2013 (UTC)
>
> > I work in Account creation, and I see personal info in almost every request. As an identified editor, I had no problem with the scanned ID, and will happily do it again. A symbolic paypal payment is also acceptable. I don't think a postcard would work for me. I live in a remote area and sometimes I get mail 2-3 months late. (although I have no problem with that as long as that is taken into account) I am worried a bit that there will soon be an admin requirement for this. I don't want to be an admin, but more and more I am finding that it is necessary to become an admin just so that I can do the things I do on Wikipedia. --Sue Rangell (talk) 19:42, 2 November 2013 (UTC)

I agree with most comments made there

- most businesses requiring ID information record first name, last name, dob, country-region-date for issuing the ID document, and unique number of the document. They do not keep a copy of the ID but usually ask to "see" the ID paper and record data themselves in front of you. Ideally, it would be a declaration of honour you would require from us. Alternatively, we sent (in some encrypted fashion if possible) the scan, you record the data and you delete the scan.
- I recently moved; wrote my US bank to record the new postal address; they wrote to my former address for confirmation and ask me to send back a document. Very simple way to check addresses. Easy to do the same with the email address for confirmation. May be renewed once a year if suitable (as in… once a year, WMF send a new year eve wish card to all its agents and agents have to answer "thank you" :))
- Token payment is an option as well
- and yes, please rely on cases where people are or have been board members or staff within chapters (or on WMF board for that matter ;)). All those people already disclosed mandatorily their ID data to their chapters.
- use opportunities of face to face meetings to do an irl ID check-up (wikimania, wikimedia events when WMF staff is there) rather than electronic one.

Anthere (talk) 10:24, 7 November 2013 (UTC)

Statement from user:aschmidt

The following discussion is closed: ***Closing given how long it has been since the last edits and the large changes on the draft since then. Will archive in a couple days unless reopened. Jalexander--WMF 20:52, 9 December 2013 (UTC)***

One of the most fundamental priciples in data-protection law is that no data shall be collected and saved unless it is absolutely necessary to do so. There is no point in collecting scans of OTRS sysops' and maybe even agents' official documents. If the WMF is interested in learning who works in OTRS it would suffice to store their names and adresses only. This is why it would be disproportionate to keep any scans. For the same reason there is no legal justification for keeping all this data for years after a Wikipedian has ceased to contribute to OTRS.

To put it clearly: The Wikimedia Foundation is a big U.S. foundation worth millions of Dollars that runs hundreds of huge websites in some 200 languages. Those volunteering in the OTRS team provide online support for free that the Foundation would otherwise have to pay for by hiring agents. When I contribute for free as a volunteer to OTRS I expect the WMF to except us from any liability whatsoever as long as we are acting in good faith. Also, I think it is not only a matter of whether only OTRS sysops or agents, too, should be subject to this new policy. If it would be enacted I would quit German-language OTRS even as an ordinary agent.--Aschmidt (talk) 19:30, 28 October 2013 (UTC)

> Hi Aschmidt! Thank you for your sharing your feedback. I'd like to hear more about what concerned you about this draft. We are trying to change this draft such that it gets to a point that most people are comfortable with its requirements. We certainly are not trying to drive you away from being an OTRS agent!
>
> First, do you believe that WMF should keep any kind of identification policy at all, as discussed above? If we do continue to have an identification policy, you mentioned that you think real names and addresses would suffice. Did you mean email address or physical addresses? What way would you feel comfortable submitting that information? Do you think that information should be verified in a particular way?
>
> You have also indicated that you believe retention of such information for 3 years following the retirement of access rights is too long. What would be a more appropriate retention period in your eyes? There has been a more detailed discussion about this particular topic above that might interest you.
>
> And finally, if we do retain an identification policy of some kind, do you believe that OTRS agents should be subject to it (assuming that the policy adequately addresses your other concerns)? Why or why not?
>
> Thanks again for taking the time to help us make this policy draft better. Mpaulson (WMF) (talk) 18:35, 30 October 2013 (UTC)

Stuff to think about

The following discussion is closed: ***Closing given how long it has been since the last edits and the large changes on the draft since then. Will archive in a couple days unless reopened. Jalexander--WMF 20:53, 9 December 2013 (UTC)***

Just to make clear, I do not wish to reidentify if this policy becomes live. I identified when people could still go to a local WMF office and then make themselves clear for a local WM office member, and so identify themselves. I send my ID two years ago and then it was destroyed and only a few basic stuff were needed (name, date of birth, nationality etc). I cannot believe that rewriting an exisiting policy which works fine for over six years is more important than improving existing tools and developing new tools for the hardworking community. You even make it harder for the volunteers to do their work. Also I'm not comfortable with the WMF keeping my ID somewhere in the USA, or even with some basic information. You know who I am. That should be enough. You should spend time at the tools we actually need (finalizing SUL, global rename, global checkuser, global blocking etc) instead of writing new fancy tools such as wikilove, the thank button and visual editor. I know it's important to attract new volunteers, but please do your best to keep the existing ones as well. FYI, I'm one of the most active stewards and meta CUs and the active CU on commons. It's your loss if I quit, not mine. I have enough useful things to do. And I know more people think about this the same as I do. Some might say: "well, those are the consequences if you change a policy. Approximately 10% quits." But I disagree with that. You should listen to the people who do the work. And do something with their feedback. I'm also waiting for three months almost for an answer of Philippe (unrelated to this). That illustrates how the staff works here with the volunteers I guess. It's easy to answer easy questions, but less easy to answer to more difficult questions apparantly. Thanks for your time. (And don't get me wrong, I am happy with some things, though not with everything...) Regards, Trijnstel$_{talk}$ 12:24, 3 November 2013 (UTC)

> Hi Trijnstel - Thanks for your comments, which definitely resonate with me. We actually take the feedback from volunteers in these consultations quite seriously - and modify or propose ideas accordingly. I agree that, if we require improved identification, we probably should explore avoiding a new identification with the same information. In response to the feedback, one proposal - which we make above - is to eliminate all identification requirements, and that would address some of your concerns, I believe, and in fact render the job of volunteers a bit less administrative. I'm sorry about the lack of response for one inquiry. If you resend your question to me, I will try to get someone to handle it for you. I completely agree that your quitting is our lose ... so please don't. :) Our volunteers are so critical to the movement and its mission. Without any exaggeration, you are the inspiration for all of us. Geoffbrigham (talk) 00:41, 6 November 2013 (UTC)
>
> > Hi Geoff. Thanks for answering. Here a follow-up as I don't really get what you mean. You say:
> >
> > - *"if we require improved identification, we probably should explore avoiding a new identification with the same information"* - so that would mean that the re-identification rule would still apply in the new policy (with the 3 year retention in it), but what do you mean with "new identification with the same information"? Saving name, age etc? (which I'm not fond of either)
> > - *"one proposal - which we make above - is to eliminate all identification requirements"* - so everyone can identify then? Even if you're not yet 18 or 21 (depends in which country you live)? That's a really bad idea imho. And it doesn't address my concerns at all, which is that the Wikimedia Foundation will keep the ID of the volunteers who just want to help. With the posibility to sue them if they do something wrong, instead of making the WMF responsible. Or maybe I didn't understand you correctly?
> >
> > > Sorry, I was not that clear after thinking about your question some more. I agree with you in principle that we need to minimize the burden of identification and reidentification on our volunteers. So I'm open to an easier re-identification procedure where we retain the basic information (name, date of birth, point of contact). With known volunteers, we could figure out simple ways to get that information to hopefully decrease the administrative burden. I do think that, if we require identification, we would need to record the name, date of birth, and contact information to be consistent with the intent of the applicable Board resolution. We do not need to keep the identification, but we do need to record the identifying information to be honest by the Board resolution.
> > > If we eliminated the identification process at WMF, we would simply rely on the community processes to properly vet volunteers per the age requirements and capabilities; that way WMF would be retaining no personal information on our volunteers. (After reading the full consultation, that is an approach I'm beginning to consider seriously, though we would need the WMF Board to agree.)
> > > As to responsibility of the users, we could put limits on the liability, which I discuss a bit more here. To be clear, it is a hard case to imagine where we would ever sue a legitimate volunteer who is acting in good faith. My concern is about someone who, in bad faith, for example sells nonpublic information for personal gain. That is the "test" case that I'm trying to figure out. As I say, I discuss this a little more here. Thanks for the great questions and expressing your legitimate concerns, which I take quite seriously. Geoffbrigham (talk) 23:47, 6 November 2013 (UTC)
> > >
> > > > But then would local communities be responsible for handling private information? On English Wikipedia, ArbCom does vet volunteers, but I would feel uncomfortable with them having my personal info. On Commons/Wikidata/Meta etc. it's just a vote by the community. **--Rschen7754** 09:07, 7 November 2013 (UTC)
> > > >
> > > > > Under the proposed approach, I think it would be up to each community to decide what the acceptable standard would be and whether identification would be required. The number of questions that have arisen with respect to WMF holding the information and frankly the arguable ease by which one might be able to submit a fraudulent ID suggest to me that we should seriously consider eliminating all WMF identification. We would need to be clear in the privacy policy that WMF cannot identify those who have access to nonpublic information but

> > > that communities are free to set their own standards, including identification processes. We could set minimum standards, such as requiring those with access to keep the information confidential (even if they are not identified). It is not a robust approach, but, if I am reading the discussion fairly, most in this community consultation seem to be rejecting a strong verification, accountability system that is manageable in a practical way, which is fine as long as we are honest about it in the privacy policy. Geoffbrigham (talk) 19:45, 22 November 2013 (UTC)
>
> Btw, no need to look at my question, Maggie said a few days ago that she would take care of it. Trijnstel$_{talk}$ 16:33, 6 November 2013 (UTC)
>
> > Thanks, let me know if you need anything there. Geoffbrigham (talk) 23:47, 6 November 2013 (UTC)

WMF board, FDC, etc.

The following discussion is closed: ***Closing given how long it has been since the last edits will archive in a couple days unless reopened Jalexander--WMF 20:54, 9 December 2013 (UTC)***

I assume that candidates for the WMF board, FDC, etc. would have to identify regardless of what is decided here - is that correct? --**Rschen7754** 09:28, 6 November 2013 (UTC)

> Correct. Geoffbrigham (talk) 20:06, 22 November 2013 (UTC)

> That would be my understanding under the inescapable international requirement to meet money laundering regulations. Both trustees on the WMF board (once elected) and FDC members have influence over the disposition and management of significant funds. I would support some form of independent but legally meaningful identification (it does not have to be through the WMF) for anyone in any Wikimedia organization taking a direct part in how significant funds are spent. Saying this, I think there is room for less onerous requirements for "insignificant" funds, such as being on a judging panel for prizes but not in control of the budget allocated, where the total being given away is less than $1,000. In those circumstances the fact that Wikimedia *should* always default to open processes, means that if someone starts giving their mates prizes in an arbitrary way, or the competition was not properly promoted so only someone's pals even take part, then at some point there will be public complaints; knowing this, anyone that fiddles the system for small amounts of money would be pretty daft and find themselves having to pay the money back. I have put "should" in italics here as I have recently found myself arguing the case for openness within Wikimedia organizations in situations I never expected and sadly find myself becoming more jaded over time with the ability of our community to implement this theoretical ideal. --Fæ (talk) 16:41, 6 November 2013 (UTC)

Pedantic lawyerly point about use of "age of majority"

The following discussion is closed: ***Closing given how long it has been since the last edits and large changes in draft since then. Will archive in a couple days unless reopened Jalexander--WMF 20:55, 9 December 2013 (UTC)***

The current policy refers to the user being "over the age at which they are capable to act without the consent of their parent in the jurisdiction in which they reside." The proposed policy instead refers to the user being "at least the age of legal majority under the laws of the jurisdiction in which they reside." I would suggest that the existing wording (or other similar wording) is preferable because it corresponds more precisely with the expressed purpose of the age requirement, viz. ensuring that users with access to sensitive information have "legal accountability" for their actions. Let me illustrate by reference to New Zealand law. The age of majority in New Zealand is technically 20 (Age of Majority Act 1970, s 4(1)).[3] (http://www.legislation.govt.nz/act/public/1970/0137/latest/DLM396495.html) However, 18 and 19 year-olds are fully legally accountable for their actions and their parents have no legal authority over them. Contracts can be enforced against them (see the definition of "minor" in the Minors' Contracts Act 1969, s 2(1)).[4] (http://www.legislation.govt.nz/act/public/1969/0041/latest/DLM392356.html) So the proposed policy would seem to exclude 18 and 19 year-olds in New Zealand, despite this being completely unnecessary in terms of the rationale.

> Interesting point. If someone is 18 or 19 in New Zealand, can they enter into a binding contract by themselves without a parental cosignatory? Geoffbrigham (talk) 22:08, 15 November 2013 (UTC)
>
> > Yes, since the Minors' Contracts Act doesn't apply to them. I recall that when I went to university aged 17 I had to have a parent sign the contracts, but when I turned 18 I was able to sign them without a parental cosignatory. Neljack (talk) 12:37, 18 November 2013 (UTC)

I apologise for raising such a technical point, but it is what we lawyers are here for, isn't it? :) Neljack (talk) 11:30, 10 November 2013 (UTC)

> Oh and while I'm at it I suppose I may as well raise a couple of other unclear points that have just occurred to me. Firstly, would the copy of the ID need to be notarised (by a lawyer, Justice of the Peace, etc)? Secondly, I don't have a government photo ID. What would happen in such cases? Neljack (talk) 11:51, 10 November 2013 (UTC)
>
> > Hi Neljack! The age of majority language has been removed from the current draft. Hopefully, that resolves this issue. Mpaulson (WMF) (talk) 23:11, 3 December 2013 (UTC)

> The proposed policy would not need a notarized document, though it would require a government photo ID. We are thinking about proposing another version of this policy, and I guess we could think about adding an alternative identification procedure. What would you suggest? We have also suggested that maybe we simply ditch this policy. What do you think about that? Geoffbrigham (talk) 22:08, 15 November 2013 (UTC)
>
> > There is no government photo ID in the UK as has already been highlighted above along with some alternative suggestions for process. I think by now that a clear majority of unpaid volunteers participating here are concerned or alarmed about the WMF holding onto their ID. Perhaps you would like to see a !vote if that is ambiguous? --Fæ (talk) 03:54, 16 November 2013 (UTC)
> > I think it would be perfectly reasonable for the Foundation to retain the information provided the documents aren't kept, though I have no objection to ditching the policy if that is considered appropriate. As for alternative forms of disclosure, I suppose if somebody required me to prove my identity I would send them a copy of my birth certificate, possibly accompanied by a statutory declaration (witnessed by a Justice of the Peace or lawyer) affirming (on pain of criminal penalties) that it is my certificate. Neljack (talk) 13:09, 18 November 2013 (UTC)
> >
> > > Hi Neljack. The ID requirement has been removed from the current draft of the policy. Thank you for taking the time to share your thoughts on the draft! Mpaulson (WMF) (talk) 23:11, 3 December 2013 (UTC)

Community Committees

The following discussion is closed: ***Closing per comment from Michelle at end. Will archive in a couple days unless reopened. Jalexander--WMF 18:38, 11 December 2013 (UTC)***

Hi, as an OTRS administrator, I would be affected by the policy proposal since it stipulates several changes to the identification procedure. As an affected user, I would like to emphasize a point others have already raised (embedded in wider critiques), which, to me, is by far the most disturbing aspect of the policy proposal. According to the proposed text of the access to nonpublic information policy (henceforth "Policy"), "[s]ometimes, the Wikimedia Foundation or a user community committee will need to contact a community member who formerly had access rights about his or her usage of those rights. For example, the Arbitration Committee may need to complete an ongoing case they are examining [...]" I would like to express my strong opposition to this. As I cannot conceive of any legal reason that would require a disclosure to a "community committee," I am puzzled as to why the Wikimedia Foundation would consider that a necessary or, for that matter, acceptable use of my data.

First, it does not fit into the overall approach of the Policy. At least members of the Election Committee and OTRS administrators do not in their respective roles participate in community processes on individual Wikimedia Wikis. It is therefore not plausible that identifying information about members of either group is passed to community committees for undoubtedly they have no competence to investigate issues that arise within the affected users' capacity as members of these groups in first place. The passing of identifying information about members of these groups to community committees can never serve to fulfill the explicit intent of the identification process ("This helps to increase accountability and ensure against misuse of information entrusted to community members with access to nonpublic information."): Whenever identifying information about such member is provided to a community committee, that must necessarily be related to a member's action unrelated to their treatment of nonpublic information; this cannot be in the spirit of the Policy.

Second, the term/phrase "community committee" is not defined in the Policy and, as far as I am aware, not elsewhere. As of now, the German-language Wikipedia's adaption of the English Wikipedia's Arbitration Committee (the *Schiedsgericht)* does not require members to be identified to the Foundation, and the scope of the two committees' activities differs considerably. Furthermore, there are ad-hoc committees for certain tasks, such as evaluating contests or organizing local elections. In light of this, it is not possible for me to understand, based on the Policy, which "committees" qualify as "community committees" within the meaning of the Policy.

Third, it is not possible at a reasonable effort for members of affected user groups to assess the risk of an undesired use of identifying data by community committees. The Wikimedia Foundation is committed to certain goals and ideals and also has a history of being transparent about internal staff policies. When a member of an affected user group releases identifying information to the Foundation, they can place some trust in the Foundation to process/store/use the information in a responsible manner. They can also keep track of the development of the Foundation and decide if they still desire to provide the Foundation with the identifying information. However, it is entirely impossible to keep track of changes to the composition or policies of community committees in hundreds of Wikimedia Wikis. If a community committee on the Italian-language Wikipedia requests identifying information about me from the Foundation and the Foundation provides the information (be it justified or not), the identifying information gets into the hands of users unknown to me and potentially unknown to the Foundation, residing somewhere in the world. This is unacceptable. Under the current phrasing, providing the Foundation with identifying information is tantamount to providing it with the competence to provide it to third parties effectively free to use the information for purposes other than those envisaged in this Policy. — Pajz (talk) 16:48, 16 October 2013 (UTC)

1. +1 There is a long history of issues with emails sent with an expectation of remaining private or confidential later being released or leaked without permission one way or another when managed by community controlled lists and archives. This does not inspire confidence for how identifying private records would be respected under this policy and the systems being proposed. --Fæ (talk) 16:10, 18 October 2013 (UTC)
2. strong +1 as well. Why would personal information about an OTRS member be disclosed to community members often anonymous. That escapes me. Anthere (talk)

Hi Pajz, Fae, and Anthere! I fear there has been a miscommunication. WMF would not disclose information from the submitted identification documents to other volunteers. Under the applicable clause in this draft, "The Wikimedia Foundation will not share submitted materials with third parties, unless such disclosure is (A) permitted by a non-disclosure agreement approved by the Wikimedia Foundation's legal department; (B) required by law; (C) needed to protect against immediate threat to life or limb; or (D) needed to protect the rights, property, or safety of the Wikimedia Foundation, its employees, or contractors." The text in the subsection following stating: "Sometimes, the Wikimedia Foundation or a user community committee will need to contact a

community member who formerly had access rights about his or her usage of those rights. For example, the Arbitration Committee may need to complete an ongoing case they are examining or the Wikimedia Foundation may need to notify you of receipt of a legal document involving that community member." is not meant to say that we would disclose the identifying information about you to other community members. This section was meant to explain the reasons for retention of your identification information. WMF would not give your identification information to other community members in this situation. We would contact you using the information you submitted to us to let you know that ArbCom needs to get ahold of you regarding an ongoing case. Would clarifying that in the policy draft help? We could also get rid of that portion talking about community committees and ArbCom all together if it's too confusing. What do you think? Mpaulson (WMF) (talk) 18:55, 31 October 2013 (UTC)

> Perhaps adding another sentence like "In that scenario, the WMF would notify you through the information you provided to us about this, but your contact information would not be given to the community members"? --**Rschen7754** 19:05, 31 October 2013 (UTC)
>
> Yes, you do need to clarify the wording. My English comprehension has been tested as excellent, even for a native speaker, so reading this again tells me that under section D, the WMF is free to share any information it wishes with any (unnamed) third party to protect its property or rights. In legal parlance, the unqualified terms "property" and "rights" are so wide as to accommodate virtually anything, including weird stuff of potential rather than defined value like reputation of the Wikimedia projects or the WMF "brand", disputed domain name registrations, or disputed claims of copyright of its materials or future "community logos". To emphasise the point, "third parties" means *anyone*. --Fæ (talk) 19:25, 31 October 2013 (UTC)
>
> Dear Michelle, thank you for your detailed response. I would certainly appreciate a clarification in the draft, though I am indifferent as to whether that should take the form of a removal of the passage about community committees alltogether or a rephrasing in the spirit of Rschen7754's proposal above; as for me, I cannot conceive of a reason why a community committee would need to reach identified users through these means. If a user is ready to answer questions from community committees, they won't have a problem reaching him; if he does not leave contact information and does not react to posts on his talk page, odds are that he just doesn't wish to be involved in Wikipedia or Wikimedia matters anymore. And while these committees play a vital role in our community, they are not ultimately conducting legally relevant investigations, so why bother identified volunteers? But as I said, I don't really care about that as long as the Foundation doesn't pass the information to members of these committees.
> Which brings me to another passage you quote, and which Fae criticizes above. I concur with Fae's point. I'm not happy with (D) in its current form. As Fae points out, the provision is lacking any specification of the third party involved. I am sure you have given this more thought than I have, but couldn't this at least be narrowed down to law enforcement agencies? In another comment of yours, you suggest to change the wording from "(D) needed to protect the rights, property, or safety of the Wikimedia Foundation, its employees, or contractors" to "(D) needed to protect the safety of others or WMF staff, contractors, systems or property" and give the example of an identified community member breaking into your building. Earlier today, you provided another example of a volunteer who "purposefully planted any viruses, malware, worms, Trojan horses, or malicious code that could harm our technical infrastructure in violation of the Terms of Use or that could expose the personal, nonpublic information of other users." In both cases I assume that the party you would share the information with is a police agency and/or a state attorney (I presume this varies among different legal systems). This suggests to me that you could narrow down the third party recipients of the information as proposed. I do have some other criticism with respect to the points (A)–(D), but I do think that a specification of "third party" would be a grave improvement anyway. I would be interested in your thoughts on this. Regards, — Pajz (talk) 23:01, 31 October 2013 (UTC)
>
> > Hi Pajz. I understand your concern regarding the term "third party" in relation to subsection (D)(i). We are currently reevaluating that section in light of community feedback and will be responding accordingly in a thread below. Because the community committees topic has been resolved, we are going to close this thread and continue the discussion about which scenarios sharing submitted materials would be appropriate in the other thread. Thank you for your feedback and patience! Mpaulson (WMF) (talk) 00:17, 10 December 2013 (UTC)

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 10

OTRS Open Technology Real Services

Redacted

Global exception request

printed by James Alexander (jalexander@wikimedia.org), 04/11/2018 21:49:27

State	closed successful	**Age**	1661 d 10 h
Priority	3 normal	**Created**	09/23/2013 11:06:06
Queue	stewards		
Lock	lock		
CustomerID	Redacted@wikimedians.ca		
Owner	Jamesofur (James Alexander)		

Article #1

From: Redacted @wikimedians.ca>
To: stewards@wikimedia.org
Subject: Global exception request
Created: 09/23/2013 11:06:06 by customer
Type: email-external

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Hi! I was referred to meta[1] when I whinged about not being able to
edit from my currently-preferred browser, which utilizes TOR amongst
other privacy precautions.

I am a US citizen living abroad. According to recent news reports this
places me in a category for elevated surveillance by my government,
despite such surveillance of its citizens actually being illegal under
US law. I prefer to minimize such invasions of my privacy and so use
TOR where possible. The global block on TOR exit points has reduced my
spontaneous contributions to the WMF projects I am still somewhat
involved with. I believe I would contribute more if, when I see
something to fix, I could simply log in and edit rather than log in,
attempt to edit, get told I'm blocked, load a different browser and
navigate to the page I wish to edit, log in again, and finally make
the change.

I believe I am a wikimedian in good standing, with a moderate history
of involvement with WMF and with the WMF projects, and am unlikely to
engage in grossly inappropriate behaviour (other than, perhaps,
discussions regarding WMF trademark practices.)

Regards,

Redacted

P.S. Oh, I'm Redacted everywhere... obviously it's the username I'd
prefer to use (and if any of you would be willing to just usurp that
darned Italian login I made waaaaaaaay long time ago so I could
finally achieve SUL, I'd appreciate that, too. Yah, I've tried to get
it through the it.WP bureaucrats a couple of times.)

[1]
https://meta.wikimedia.org/wiki/No_open_proxies#Global_exceptions_and_appeals
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.12 (GNU/Linux)
Comment: Using GnuPG with Thunderbird - http://www.enigmail.net/

Redacted
-----END PGP SIGNATURE-----
```

Article #2

From: Wikimedia stewards <stewards@wikimedia.org>
To: Redacted@wikimedians.ca
Subject: Re: [Ticket# Redacted] Global exception request
Created: 09/23/2013 11:17:20 by agent
Type: email-external

OTRS Open Technology Real Services

Redacted

Gday Redacted

Did the global IP block exemption.

Re the account, when they do their global account reconciliation you will get the global account and the other will be renamed, so leaving it and letting it happen is the best management means.

Regards, sDrewth

Wikimedia Stewards

Disclaimer: all mail to this address is answered by volunteers, and responses are not to be considered an official statement of the Wikimedia Foundation. For official correspondence, please contact the Wikimedia Foundation by certified mail at the address listed on <https://www.wikimediafoundation.org/>

23/09/2013 11:06 - Redacted wrote:

> -----BEGIN PGP SIGNED MESSAGE-----
> Hash: SHA1
>
> Hi! I was referred to meta[1] when I whinged about not being able to
> edit from my currently-preferred browser, which utilizes TOR amongst
> other privacy precautions.
>
> I am a US citizen living abroad. According to recent news reports this
> places me in a category for elevated surveillance by my government,
> despite such surveillance of its citizens actually being illegal under
> US law. I prefer to minimize such invasions of my privacy and so use
> TOR where possible. The global block on TOR exit points has reduced my
> spontaneous contributions to the WMF projects I am still somewhat
> involved with. I believe I would contribute more if, when I see
> something to fix, I could simply log in and edit rather than log in,
> attempt to edit, get told I'm blocked, load a different browser and
> navigate to the page I wish to edit, log in again, and finally make
> the change.
>
> I believe I am a wikimedian in good standing, with a moderate history
> of involvement with WMF and with the WMF projects, and am unlikely to
> engage in grossly inappropriate behaviour (other than, perhaps,
> discussions regarding WMF trademark practices.)
>
> Regards,
>
> Redacted
>
> P.S. Oh, I'm Redacted everywhere... obviously it's the username I'd
> prefer to use (and if any of you would be willing to just usurp that
> darned Italian login I made waaaaaaaay long time ago so I could
> finally achieve SUL, I'd appreciate that, too. Yah, I've tried to get
> it through the it.WP bureaucrats a couple of times.)
>
> [1]
> https://meta.wikimedia.org/wiki/No_open_proxies#Global_exceptions_and_appeals
> -----BEGIN PGP SIGNATURE-----
> Version: GnuPG v1.4.12 (GNU/Linux)
> Comment: Using GnuPG with Thunderbird - http://www.enigmail.net/
>
> Redacted
> -----END PGP SIGNATURE-----
>
>

Article #3

From:	Wikimedia stewards <stewards@wikimedia.org>
To:	apalmer@wikimedia.org
Subject:	Fwd: [Ticket# Redacted Global exception request
Created:	04/03/2018 23:24:05 by agent
Type:	email-external

Yours sincerely,
James Alexander

Wikimedia Stewards

Disclaimer: all mail to this address is answered by volunteers, and responses are not to be considered an official statement of the Wikimedia Foundation. For official correspondence, please contact the Wikimedia Foundation by certified mail at the address listed on <https://www.wikimediafoundation.org/>
---- Forwarded message from Redacted @wikimedians.ca> ---

From: Redacted @wikimedians.ca>

OTRS Open Technology Real Services

Redacted

To: stewards@wikimedia.org
Subject: Global exception request
Date: 09/23/2013 11:06:06

> -----BEGIN PGP SIGNED MESSAGE-----
> Hash: SHA1
>
> Hi! I was referred to meta[1] when I whinged about not being able to
> edit from my currently-preferred browser, which utilizes TOR amongst
> other privacy precautions.
>
> I am a US citizen living abroad. According to recent news reports this
> places me in a category for elevated surveillance by my government,
> despite such surveillance of its citizens actually being illegal under
> US law. I prefer to minimize such invasions of my privacy and so use
> TOR where possible. The global block on TOR exit points has reduced my
> spontaneous contributions to the WMF projects I am still somewhat
> involved with. I believe I would contribute more if, when I see
> something to fix, I could simply log in and edit rather than log in,
> attempt to edit, get told I'm blocked, load a different browser and
> navigate to the page I wish to edit, log in again, and finally make
> the change.
>
> I believe I am a wikimedian in good standing, with a moderate history
> of involvement with WMF and with the WMF projects, and am unlikely to
> engage in grossly inappropriate behaviour (other than, perhaps,
> discussions regarding WMF trademark practices.)
>
> Regards,
>
> Redacted
>
> P.S. Oh, I'm Redacted everywhere... obviously it's the username I'd
> prefer to use (and if any of you would be willing to just usurp that
> darned Italian login I made waaaaaaaay long time ago so I could
> finally achieve SUL, I'd appreciate that, too. Yah, I've tried to get
> it through the it.WP bureaucrats a couple of times.)
>
> [1]
> https://meta.wikimedia.org/wiki/No_open_proxies#Global_exceptions_and_appeals
> -----BEGIN PGP SIGNATURE-----
> Version: GnuPG v1.4.12 (GNU/Linux)
> Comment: Using GnuPG with Thunderbird - http://www.enigmail.net/
>
> Redacted
> -----END PGP SIGNATURE-----
>
>
---- End forwarded message ---