

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 4 OF 7 (JA2353–JA2889)

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

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 Defendants–Appellees

*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

U.S. District Court for the District of Maryland, Docket Sheet,
Case No. 1:15-cv-00662JA0001

Plaintiff Wikimedia Foundation’s Amended Complaint
(June 22, 2015), ECF No. 72JA0036

Exhibits to Wikimedia Foundation’s Motion to Compel

Declaration of Patrick Toomey, Counsel for Wikimedia Foundation
(Mar. 26, 2018), ECF No. 125-3JA0096

Exhibit 1: Chart Identifying Discovery Requests at Issue on
Wikimedia Foundation’s Motion to Compel,
ECF No. 125-4.....JA0101

Exhibit 2: Wikimedia Foundation’s Requests for Admission
and attachments (Nov. 7, 2017), ECF No. 125-5.....JA0118

**Exhibits to Defendants’ Opposition
to Wikimedia Foundation’s Motion to Compel**

Declaration of Daniel R. Coats, Director of National Intelligence
(Apr. 28, 2018), ECF No. 138-2.....JA0170

Declaration of Lauren L. Bernick, Senior Associate Civil Liberties
Protection Officer in the Office of Civil Liberties, Privacy, and
Transparency at the Office of the Director of National Intelligence
(Apr. 28, 2018), ECF No. 138-3.....JA0190

Notice of Filing Unclassified & Redacted Version of the Declaration of George C. Barnes, Deputy Director of the NSA (May 11, 2018), ECF No. 141JA0199

Unclassified & Redacted Version of the Declaration of George C. Barnes, Deputy Director of the NSA (May 11, 2018), ECF No. 141-1JA0201

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

Declaration of Ashley Gorski, Counsel for Wikimedia Foundation (May 18, 2018), ECF No. 143-1JA0270

Exhibit 1: Chart Identifying Deposition Questions at Issue on Wikimedia Foundation’s Motion to Compel, ECF No. 143-2.....JA0272

Exhibit 2: Transcript of Deposition of NSA’s Designated Witness, Rebecca J. Richards, Pursuant to Fed. R. Civ. P. 30(b)(6) (Apr. 16, 2018), ECF No. 143-3JA0286

**Opinion & Order
Denying Wikimedia Foundation’s Motion to Compel**

Memorandum Opinion (Aug. 20, 2018), ECF No. 150.....JA0689

Order Denying Plaintiff’s Motion to Compel Discovery Responses & Deposition Testimony (Aug. 20, 2018), ECF No. 151.....JA0716

Exhibits to Defendants’ Motion for Summary Judgment

Declaration of Henning Schulzrinne, Julian Clarence Levi Professor of Computer Science at Columbia University (Nov. 13, 2018), ECF No. 164-4.....JA0719

Declaration of James Gilligan, Counsel for Defendants (Nov. 13, 2018), ECF No. 164-5JA0818

Exhibit 3: Wikimedia Foundation’s Amended and Supplemental Responses and Objections to NSA’s First Set of Interrogatories (Mar. 23, 2018), ECF No. 164-6JA0821

Exhibit 4: Wikimedia Foundation’s Amended Responses and Objections to ODNI’s Interrogatory No. 19 (Apr. 6, 2018), including Technical Statistics Chart, ECF No. 164-7JA0861

Exhibit 5: Wikimedia Foundation’s Responses and Objections to NSA’s First Set of Interrogatories (Jan. 11, 2018), ECF No. 164-8.....JA0876

VOLUME 2

**Exhibits to Wikimedia Foundation’s
Opposition to Defendants’ Motion for Summary Judgment**

Declaration of Scott Bradner, Former Senior Technology Consultant for the Harvard University Chief Technology Officer (Dec. 18, 2018), ECF No. 168-2JA0920

Appendices A through Z to Declaration of Scott Bradner (Dec. 18, 2018), ECF Nos. 168-3 to 168-4JA1067

VOLUME 3

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

Appendices AA through FF to Declaration of Scott Bradner (Dec. 18, 2020), ECF No. 168-5JA1791

Declaration of Jonathon Penney, Associate Professor at the Schulich School of Law and Director of the Law & Technology Institute at Dalhousie University (Dec. 18, 2018), ECF No. 168-6JA2151

Declaration of Michelle Paulson, Former Legal Director and Interim General Counsel for Wikimedia Foundation (Dec. 18, 2018), ECF No. 168-7.....JA2218

Declaration of James Alexander, Former Manager for Trust and Safety and Former Legal and Community Advocacy Manager at Wikimedia Foundation (Dec. 18, 2018), ECF No. 168-8JA2244

Declaration of Tilman Bayer, Senior Analyst for Wikimedia Foundation Product Analytics Team (Dec. 18, 2018), ECF No. 168-9.....JA2253

Declaration of Emily Temple-Wood (Dec. 18, 2018), ECF No. 168-10.....JA2268

Declaration of Patrick Toomey, Counsel for Wikimedia Foundation (Dec. 18, 2018), ECF No. 168-11.....JA2278

Exhibit 8: Wikimedia-hosted email list discussing NSA slide with Wikimedia logo, from July to August 2013, ECF No. 168-12.....JA2283

Exhibit 9: Wikimedia “Talk page” discussing its non-public information policy, from September to December 2013, ECF No. 168-13.....JA2305

Exhibit 10: “OTRS” ticket showing Wikimedia user requesting Tor permissions in September 2013, ECF No. 168-14JA2349

VOLUME 4

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

Exhibit 11: Wikimedia webpage showing Wikimedia user requesting Tor permissions in September 2017, ECF No. 168-15.....JA2353

Exhibit 12: Wikimedia document compiling German-user-

community appeal concerning privacy in 2013,
 ECF No. 168-16.....JA2357

Exhibit 13: Wikimedia “Talk page” discussing NSA
 surveillance from June to December 2013,
 ECF No. 168-17.....JA2363

Exhibit 14: Wikimedia Technical Statistics Chart & Supporting
 Exhibits A-G, ECF No. 168-18JA2396

Exhibit 15: Privacy & Civil Liberties Oversight Board, *Report
 on the Surveillance Program Operated Pursuant to Section 702
 of FISA* (July 2014), ECF No. 168-19.....JA2434

Exhibit 16: FISC Memorandum Opinion, [*Redacted*], 2011 WL
 10945618 (Oct. 3, 2011), ECF No. 168-20JA2631

Exhibit 17: Office of the Director of National Intelligence, *DNI
 Declassifies Intelligence Community Documents Regarding
 Collection Under Section 702 of FISA* (Aug. 21, 2013),
 ECF No. 168-21.....JA2717

Exhibit 18: Defendant NSA’s Objections and Responses to
 Plaintiff’s First Set of Interrogatories (Dec. 22, 2017),
 ECF No. 168-22.....JA2721

Exhibit 19: FISC Submission, *Clarification of National Security
 Agency’s Upstream Collection Pursuant to Section 702 of FISA*
 (May 2, 2011), ECF No. 168-23JA2743

Exhibit 20: Office of the Director of National Intelligence,
*Statistical Transparency Report Regarding Use of National
 Security Authorities, Calendar Year 2017* (Apr. 2018),
 ECF No. 168-24.....JA2748

Exhibit 21: FISC Memorandum Opinion & Order
 (Apr. 26, 2017), ECF No. 168-25.....JA2790

VOLUME 5

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

Exhibit 22: FISC Submission, *Government’s Response to the Court’s Briefing Order of May 9, 2011* (June 1, 2011), ECF No. 168-26.....JA2890

Exhibit 23: *Big Brother Watch & Others v. United Kingdom*, App. Nos. 58170/13, 62322/14, 24960/15, Eur. Ct. H.R. (2018), ECF No. 168-27.....JA2932

Exhibit 24: NSA Director of Civil Liberties & Privacy Office, *NSA’s Implementation of FISA Section 702* (Apr. 16, 2014), ECF No. 168-28.....JA3145

Exhibit 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), ECF No. 168-29JA3157

Exhibit 26: Minimization Procedures Used by the NSA in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of FISA (July 2014), ECF No. 168-30.....JA3193

Exhibit 27: Glenn Greenwald, *XKeyscore: NSA Tool Collects “Nearly Everything a User Does on the Internet,”* Guardian, July 31, 2013, ECF No. 168-31JA3209

Exhibit 28: NSA slide, excerpted from Exhibit 27 (Greenwald, *XKeyscore: NSA Tool Collects “Nearly Everything a User Does on the Internet”*), ECF No. 168-32JA3220

Exhibit 29: Morgan Marquis-Boire, et al., *XKEYSCORE: NSA’s Google for the World’s Private Communications*, Intercept, July 1, 2015, ECF No. 168-33JA3222

Exhibit 30: NSA slide deck, *XKEYSCORE for Counter-CNE*, published in The Intercept on July 1, 2015, ECF No. 168-34 ...JA3237

Exhibit 31: Wikimedia, *Founding Principles*
 (accessed Mar. 14, 2018), ECF No. 168-35JA3259

Exhibit 32: Yana Welinder, *Opposing Mass Surveillance on the Internet*, Wikimedia Blog (May 9, 2014), ECF No. 168-36JA3262

Exhibit 33: Wikimedia Public Policy, *Privacy*
 (accessed Mar. 14, 2018), ECF No. 168-37JA3266

Exhibit 34: Wikipedia, *Sock Puppetry*
 (accessed Mar. 14, 2018), ECF No. 168-38JA3273

Exhibit 35: Wikimedia, *Privacy Policy*
 (accessed Feb. 14, 2018), ECF No. 168-39.....JA3286

Exhibit 36: Ryan Lane, *The Future of HTTPS on Wikimedia Projects*, Wikimedia Blog (Aug. 1, 2013),
 ECF No. 168-40.....JA3311

Exhibit 37: Yana Welinder, et al., *Securing Access to Wikimedia Sites with HTTPS*, Wikimedia Blog
 (June 12, 2015), ECF No. 168-41JA3317

Exhibit 38: Wikimedia email describing Tech/Ops goals and
 the importance of HTTPS (May 23, 2014), ECF No. 168-42....JA3325

Exhibit 39: Wikimedia document discussing IPsec
 implementation, including July 8, 2013 statement from a
 Wikimedia engineer, ECF No. 168-43JA3328

Exhibit 40: Wikimedia job posting for Traffic Security
 Engineer (accessed Feb. 8, 2018), ECF No. 168-44JA3364

Exhibit 41: Michelle Paulson, *A Proposal for Wikimedia’s New Privacy Policy and Data Retention Guidelines*, Wikimedia
 Blog (Feb. 14, 2014), ECF No. 168-45JA3367

Exhibit 42: Wikimedia’s Supplemental Exhibit C in response

to NSA Interrogatory No. 8 (volume of HTTP border-crossing communications by country), ECF No. 168-46JA3375

Exhibit 43: Wikimedia’s Supplemental Exhibit D in response to NSA Interrogatory No. 8 (volume of HTTPS border-crossing communications by country), ECF No. 168-47JA3388

Exhibit 44: Wikimedia analytics document showing monthly unique visitors to Wikimedia by region, from December 2007 to May 2015, ECF No. 168-48JA3400

Exhibit 45: Press Release, NSA, *NSA Stops Certain Section 702 “Upstream” Activities*, Apr. 28, 2017, ECF No. 168-49.....JA3404

VOLUME 6

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

Second Declaration of Henning Schulzrinne, Julian Clarence Levi Professor of Computer Science at Columbia University (Feb. 15, 2019), ECF No. 178-2JA3407

Declaration of Alan J. Salzberg, Principal of Salt Hill Statistical Consulting (Feb. 15, 2019), ECF No. 178-3JA3452

Second Declaration of James Gilligan, Counsel for Defendants (Feb. 15, 2019), ECF No. 178-4JA3725

Exhibit 9: Wikimedia Foundation’s Responses and Objections to DOJ’s First Set of Interrogatories (Jan. 11, 2018), ECF No. 178-5.....JA3728

Exhibit 10: Relevant Portions of the Deposition of James Alexander, Wikimedia Foundation witness taken pursuant to Fed. R. Evid. 30(b)(6), ECF No. 178-6JA3761

Exhibit 11: Relevant Portions of the Deposition of Michelle

Paulson, Wikimedia Foundation witness taken pursuant to
 Fed. R. Evid. 30(b)(6), ECF No. 178-7JA3777

Exhibit 12: Wikimedia Foundation, *Securing access to
 Wikimedia sites with HTTPS*, June 12, 2015
 (WIKI0007108-7114), ECF No. 178-8JA3791

Exhibit 13: Wikipedia: Village pump (technical)/Archive 138
 (WIKI0006872-6938), ECF No. 178-9JA3800

Exhibit 14: Jimmy Wales and Lila Tretikov, “Stop Spying on
 Wikimedia Users,” N.Y. Times, Mar. 10, 2015,
 ECF No. 178-10.....JA3869

Exhibit 15: Wikimedia Foundation, *Wikimedia v. NSA:
 Wikimedia Foundation files suit against NSA to challenge
 upstream mass surveillance*, Mar. 10, 2015,
 ECF No. 178-11.....JA3873

VOLUME 7

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

Second Declaration of Scott Bradner, Former Senior Technology
 Consultant for the Harvard University Chief Technology Officer
 (Mar. 8, 2019), ECF No. 181-1JA3879

Second Declaration of Jonathon Penney, Associate Professor at the
 Schulich School of Law and Director of the Law & Technology
 Institute at Dalhousie University (Mar. 8, 2019), ECF No. 181-2JA3940

Second Declaration of Michelle Paulson, Former Legal Director
 and Interim General Counsel for Wikimedia Foundation
 (Mar. 8, 2019), ECF No. 181-3JA4006

Second Declaration of Tilman Bayer, Senior Analyst for Wikimedia
 Foundation Product Analytics Team (Mar. 8, 2019),
 ECF No. 181-4.....JA4012

Second Declaration of Emily Temple-Wood (Mar. 8, 2019),
ECF No. 181-5JA4015

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

Third Declaration of Henning Schulzrinne, Julian Clarence Levi
Professor of Computer Science at Columbia University
(Mar. 22, 2019), ECF No. 182-2JA4019

Second Declaration of Alan J. Salzberg, Principal of Salt Hill
Statistical Consulting (Mar. 22, 2019), ECF No. 182-3JA4048

**Opinion & Order
Granting Defendants’ Motion for Summary Judgment**

Memorandum Opinion (Dec. 16, 2019), ECF No. 188JA4073

Order Granting Defendants’ Motion for Summary Judgment
(Dec. 16, 2019), ECF No. 189JA4123

Wikimedia Foundation’s Notice of Appeal

Notice of Appeal (Feb. 14, 2020), ECF No. 191JA4124

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 11

Steward requests/Global permissions

< [Steward requests](#)

This is an archived version of this page, as edited by [Rusliko](#) (talk | contribs) at 11:21, 8 September 2017. It may differ significantly from the current version.

(diff) ← Older revision | Latest revision (diff) | Newer revision → (diff)

← [Requests and proposals](#) **Steward requests** (Global permissions) [latest archive](#) →

This page hosts requests for global permissions. To make a request, read the relevant policy ([global rollback](#), [global sysop](#), [global rename](#), ...) and make a request below. Explain why membership is needed for that group, and detail prior experience or qualifications.

This is not a vote and any active Wikimedia editor may participate in the discussion.

Successful global rollback requests require no fewer than 5 days of discussion, while successful global renamer and global sysop discussions require no fewer than 2 weeks.

[Search in this page hierarchy](#)

Contents

Requests for global rollback permissions

[Global rollback for Asaf \(WMF\)](#)

Requests for global sysop permissions

Requests for global IP block exemption

[Global IP block exempt for TemTem](#)

Requests for global rename permissions

Requests for other global permissions

[remove global OTRS member for Wikitanvir](#)

[remove global OTRS member for Panyd](#)

[remove global OTRS member for Kh80](#)

[See also](#)

Cross-wiki requests

- [CheckUser information](#)
- [Global blocks/locks](#)
- [Permissions \(global\)](#)
- [Permissions \(bot\)](#)
- [Permissions \(other\)](#)
- [Username changes/ usurpation requests](#)
- [Miscellaneous requests](#)
- [URL blacklisting](#)
- [Title/username blacklisting](#)
- [Email blacklisting](#)

Meta-Wiki requests

- [CheckUser information](#)
- [Deletion](#)
- [Permissions](#)
- [Requests for help](#)

Requests for global rollback permissions

Please be sure to follow the instructions below:

Your request might be rejected if you don't follow the instructions, and not doing so would reflect poorly on your suitability. Please also review the [Global rollback policy](#).



Please note that global rollbacker discussions are not votes. Comments must present specific points in favor of or against a user's approval.

[Instructions for making a request](#)

[\[Expand\]](#)

Global rollback for Asaf (WMF)

Status: **In progress**

- Global user: [Asaf \(WMF\)](#) (edits • CA • [global groups](#) ([https://meta.wikimedia.org/wiki/Special:GlobalGroupMembership/Asaf_\(WMF\)?user-reason=%5B%5Bspecial:Permalink/17203746%5D%5D](https://meta.wikimedia.org/wiki/Special:GlobalGroupMembership/Asaf_(WMF)?user-reason=%5B%5Bspecial:Permalink/17203746%5D%5D)) • [crosswiki-ness](#) (h

Rationale: I work in many wikis, and every now and then encounter vandalism (especially on old pages I still watch), like [this](https://meta.wikimedia.org/w/index.php?title=Grants%3APEG%2FWM_CZ%2FCommunities&type=revision&diff=17194610&oldid=10953431) (https://meta.wikimedia.org/w/index.php?title=Grants%3APEG%2FWM_CZ%2FCommunities&type=revision&diff=17194610&oldid=10953431), where the rollback function would be useful. I am a longtime trusted user and staffer, and I humbly suggest there is zero risk in giving me the rollback tool so I can rollback vandalism when I encounter it, even though I'm not proactively patrolling most wikis. Also see [this discussion](https://meta.wikimedia.org/wiki/Wikimedia_Forum#Standalone_rollbacker_permission.3F) (https://meta.wikimedia.org/wiki/Wikimedia_Forum#Standalone_rollbacker_permission.3F). [Asaf \(WMF\)](#) (talk) 14:57, 6 September 2017 (UTC)

Not ending before 11 September 2017 14:57 UTC

- Do you have a community account in addition to a WMF one? [Ruslik](#) (talk) 18:42, 6 September 2017 (UTC)


Certainly. This is it. Also linked from the first line under About me on my staff account. [ljon](#) (talk) 22:46, 6 September 2017 (UTC)

I think you should request global rollback for your volunteer account. We are not in business here assigning permissions to staff accounts. If you want it for your staff account, you should ask someone in WMF. [Ruslik](#) (talk) 20:29, 7 September 2017 (UTC)


- I was under the impression that staff were supposed to keep non-work-related edits to articles to volunteer accounts, including reverting vandalism. Is that correct? --[Rschen7754](#) 00:13, 7 September 2017 (UTC)

yes, that is correct. I suppose the global rollback tool would be useful to them on both accounts. The example diff above is on an old page, which I watch in my staff capacity, so I think rolling back the vandalism would have been fine under my staff account. I may well encounter random vandalism (say on article space) on some wiki I visit in the course of my work that would be more appropriately reverted through my volunteer account. I am happy to request separately under my volunteer account as well. Asaf (VMMF) (talk) 18:59, 7 September 2017 (UTC)

Case 1:15-cv-00662-TSE Document 168-15 Filed 12/18/18 Page 3 of 4

-  **Oppose** little to zero reverting of vandalism on smaller wiki's under the volunteer account. Not on the staff account either. Policy states the following: *For consideration, users must be demonstrably active in cross-wiki countervandalism or anti-spam activities (for example, as active members of the Small Wiki Monitoring Team) and make heavy use of revert on many wikis.* These criteria are certainly not met. [Natuur12 \(talk\)](#) 20:15, 7 September 2017 (UTC)

This is somewhat unusual case. We can make an exception. [Ruslik \(talk\)](#) 20:29, 7 September 2017 (UTC)

-  **Oppose** Given rationale applies to many users, but is still out of scope of global rollback. Sorry. --[Krd](#) 10:40, 8 September 2017 (UTC)

Requests for global sysop permissions

Please be sure to follow the instructions below:

Your request might be rejected if you don't follow the instructions, and not doing so would reflect poorly on your suitability. Please also review the [Global sysops policy](#).



Stewards

When you give someone global sysop rights, please list them on [Users with global sysop access](#) and ask them to subscribe to the [global sysops mailing list](#).



Please note that **global sysop discussions are not votes**. Comments must present **specific points in favor of or against a user's approval**.

[Instructions for making a request](#)

[\[Expand\]](#)

Requests for global IP block exemption

Please be sure to follow the instructions below:



Your request might be rejected if you don't follow the instructions. Please review [Global IP block exemption](#). **Please note:** Global IP block exemption does NOT make one immune to locally-created blocks of any sort, only *global* blocks.

[Instructions for making a request](#)

[\[Expand\]](#)

Global IP block exempt for [TemTem](#)

Status: Done

- Global user: [TemTem](#) (edits • CA • global groups (<https://meta.wikimedia.org/wiki/Special:GlobalGroupMembership/TemTem?user-reason=%5B%5BSpecial:Permalink/17203746%5D%5D>) • [crosswiki-ness](https://toc.crosswiki-ness) (<https://toc>))

Hello, I would like to use Tor while editing Wikimedia wikis, but it seems Wikimedia blocks all Tor exit nodes. I have to use Tor because the country where I live in, the Philippines, is under a "War on Drugs". Martial law is also declared in Mindanao, and still in effect. I am concerned that my government 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. Thanks, --[TemTem \(talk\)](#) 00:50, 3 September 2017 (UTC)

Is this your first account? [Ruslik \(talk\)](#) 17:33, 3 September 2017 (UTC)

Yes. [TemTem \(talk\)](#) 09:38, 4 September 2017 (UTC)

Is this a joke? I have been waiting for like four days and I still have no response? You don't trust me, fine, then I will gain your trust. by editing without tor. but remove the "If a Tor exception is granted to you and you don't have an account yet, the steward will also create one for you and you'll receive a temporary password to your email address" at "No open proxies", it seems its just a fantasy. [TemTem \(talk\)](#) 10:49, 8 September 2017 (UTC)

✓ **Done** Four days is not a long time. [Ruslik \(talk\)](#) 11:21, 8 September 2017 (UTC)

Requests for global rename permissions

Please be sure to follow the instructions below:

Your request might be rejected if you don't follow the instructions, and not doing so would reflect poorly on your suitability. Please also review the [Global rename policy](#).



Stewards

When you give someone global rename rights, please add them to the list of [global renamers](#) and ask them to subscribe to the [global renamers' mailing list](#).



Please note that **global renamer discussions are not votes**. Comments must present **specific points in favor of or against a user's approval**.

[Instructions for making a request](#)

[\[Expand\]](#)

Requests for other global permissions



Please be sure to follow the instructions below:

Your request might be rejected if you don't follow the instructions.

remove global OTRS member for Wikitanvir

Status: Done

- Global user: Wikitanvir (edits · CA · global groups (https://meta.wikimedia.org/wiki/Special:GlobalGroupMembership/Wikitanvir?user-reason=%5B%5BSpecial:Permalink/17203746%5D%5D) · crosswiki-ness (https://

Thx. --Krd 10:31, 5 September 2017 (UTC)

✓ Done.--HakanIST (talk) 10:59, 5 September 2017 (UTC)

remove global OTRS member for Panyd

Status: Done

- Global user: Panyd (edits · CA · global groups (https://meta.wikimedia.org/wiki/Special:GlobalGroupMembership/Panyd?user-reason=%5B%5BSpecial:Permalink/17203746%5D%5D) · crosswiki-ness (https://tools.wmfl

Thx. --Krd 09:27, 7 September 2017 (UTC)

✓ Done.--HakanIST (talk) 09:30, 7 September 2017 (UTC)

remove global OTRS member for Kh80

Status: Done

- Global user: Kh80 (edits · CA · global groups (https://meta.wikimedia.org/wiki/Special:GlobalGroupMembership/Kh80?user-reason=%5B%5BSpecial:Permalink/17203746%5D%5D) · crosswiki-ness (https://tools.wmfl

Thx. --Krd 11:26, 7 September 2017 (UTC)

✓ Done.--HakanIST (talk) 11:39, 7 September 2017 (UTC)

See also

- User groups — Information on user groups
- Global rights log — Log of global permissions changes
- Archive
 - 2010: [03](#), [04](#), [05](#), [06](#), [07](#), [08](#), [09](#), [10](#), [11](#), [12](#)
 - 2011: [01](#), [02](#), [03](#), [04](#), [05](#), [06](#), [07](#), [08](#), [09](#), [10](#), [11](#), [12](#)
 - 2012: [01](#), [02](#), [03](#), [04](#), [05](#), [06](#), [07](#), [08](#), [09](#), [10](#), [11](#), [12](#)
 - 2013: [01](#), [02](#), [03](#), [04](#), [05](#), [06](#), [07](#), [08](#), [09](#), [10](#), [11](#), [12](#)
 - 2014: [01](#), [02](#), [03](#), [04](#), [05](#), [06](#), [07](#), [08](#), [09](#), [10](#), [11](#), [12](#)
 - 2015: [01](#), [02](#), [03](#), [04](#), [05](#), [06](#), [07](#), [08](#), [09](#), [10](#), [11](#), [12](#)
 - 2016: [01](#), [02](#), [03](#), [04](#), [05](#), [06](#), [07](#), [08](#), [09](#), [10](#), [11](#), [12](#)
 - 2017: [01](#), [02](#), [03](#), [04](#), [05](#), [06](#), [07](#), [08](#), [09](#), [10](#), [11](#), [12](#)
 - 2018: [01](#), [02](#), [03](#), [04](#), [05](#), [06](#), [07](#), [08](#), [09](#), [10](#), [11](#), [12](#)

General requests for: [help from a Meta sysop or bureaucrat](#) · [deletion](#) (speedy deletions: [local](#) · [multilingual](#)) · [URL blacklisting](#) · [new languages](#) · [interwiki map](#)

Personal requests for: [username changes](#) · [permissions](#) (global) · [bot status](#) · [adminship on Meta](#) · [an account on WMF wiki](#) · [CheckUser information](#) (local) · [local administrator help](#)

Cooperation requests for: [comments](#) (local) (global) · [translation](#) · [logos](#)

Retrieved from "https://meta.wikimedia.org/w/index.php?title=Steward_requests/Global_permissions&oldid=17203746"

Text is available under the [Creative Commons Attribution-ShareAlike License](#); additional terms may apply. See [Terms of Use](#) for details.

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 12

Handling our user data - an appeal and a response

(Today we are posting an English translation of a blog [post](#) from German Wikipedians outlining concerns about the handling of Wikipedia user data, or metadata. Above that post you will find the Foundation's response to those concerns.)

Response to user appeal

In June this year, the Wikimedia Foundation (WMF) started to solicit community input on our privacy policy, and [since September](#) we have been inviting participation in a [discussion of the draft for a new privacy policy](#). The purpose of this discussion has been to review and improve our privacy policy, and ensure that all members of the Wikimedia community have an opportunity to be heard and contribute.

This discussion has already helped us to understand the diverse range of views in our large, international community (each month, more than 75,000 users contribute to Wikimedia projects in more than 200 languages). As part of this discussion, about 120 German Wikipedia contributors who advocate for more stringent privacy rules have made a statement and published it on the German chapter's [blog](#) (English translation below). We welcome the contribution of these editors, and hope that the resulting discussion will strengthen the policy. However, while we hear and respect these concerns, the WMF was not invited to explain its position during the drafting of the statement, and so we'd like to do so here.

Existing practices

As the authors of the statement mention, the past year has seen increased global concern about privacy and the activities of intelligence agencies in [both the US and Europe](#). The Wikimedia Foundation is extremely sensitive to those concerns, and we have taken several steps to address them, [including joining activism](#) here in the US, [encrypting more traffic](#) to and from the Wikimedia sites, and [assuring readers](#) that we have not been contacted under the surveillance programs at issue.

The Wikimedia Foundation also protects its readers by collecting very little information, particularly relative to most major websites. Editors who create an account do not have to connect their account to a real-world identity unless they choose to do so. It is possible to read and use the Wikimedia sites without providing your real name, home address, email address, gender, credit card or financial information. In all but a few cases (related to abuse prevention), we delete IP addresses of logged-in editors after 90 days. All in all, there is small incentive for governments to contact WMF and request information about Wikimedia users.

Requested changes

As part of the normal operation of a wiki, the Wikimedia sites have always published certain information about edits, particularly when the edit was made, and what page was edited. This information can be collected to make educated guesses about an account, such as what time zone an account is in (based on when edits occur).

One part of the statement asks that we limit public access to this editing information. This information is used in a variety of places, many of which are important to the health and

functioning of our projects:

- Protecting against vandalism, incorrect and inappropriate content: There are several bots that patrol Wikipedia's articles that protect the site. Without public access to metadata, the effectiveness of these bots will be much reduced, and it is impossible for humans to perform these tasks at scale.
- Community workflows: Processes that contribute to the quality and governance of the project will also be affected: blocking users, assessing adminship nominations, determining eligible participants in article deletion discussions.
- Automated tools: Certain community-created tools that help perform high-volume editing (such as Huggle, for vandalism fighting on several wikis) will be broken without public access to this metadata.
- Research: Researchers around the world use this public metadata for analysis that is essential to the site and the movement's understanding of itself.
- Forking: Allowing others to fork is an important principle of the movement, and that requires some exposure of metadata about how articles were built, and by whom.

The Foundation has been open and transparent about these data publication practices for years, so we do not currently plan to make the requested changes. Nevertheless, we welcome the appeal as part of the wider community discussion regarding the Foundation's privacy policy.

The statement also asks that we implement a new policy on the Wikimedia Labs experimental development servers. The predecessor to Labs, called Toolserver, had a policy that prohibited volunteer-developed software if the software aggregated certain types of account information without consent. The terms of use for Labs allows such software to be taken down at the WMF's discretion, but does not prohibit it explicitly. We have suggested a clarification to the Labs terms of use in the Privacy Policy discussion, and will continue to discuss that there.

We invite anyone interested in Wikimedia Foundation's privacy policy to get involved in the ongoing consultation with the Wikimedia community. You can read more about that process in the blog post that announced it. The consultation process will continue through January 15, 2013.

Luis Villa

Deputy General Counsel, Wikimedia Foundation

(Translated blog post from Wikimedia Deutschland follows - from https://meta.wikimedia.org/wiki/Wikimedia_Blog/Drafts/Handling_our_user_data_-_an_appeal)

Handling our user data - an appeal

Preface (Wikimedia Deutschland)

For several months, there have been regular discussions on data protection and the way Wikimedia deals

JA2359

with it, in the German-speaking community – one of the largest non-English-speaking communities in the Wikimedia movement. Of course, this particularly concerns people actively involved in Wikipedia, but also those active on other Wikimedia projects.

The German-speaking community has always been interested in data protection. However, this particular discussion was triggered when the Deep User Inspector tool on Tool Labs nullified a long-respected agreement in the Toolserver, that aggregated personalized data would only be available after an opt-in by the user.

As the Wikimedia Foundation is currently reviewing its privacy policy and has requested feedback and discussion her by 15 January, Wikimedia Deutschland has asked the community to draft a statement. The text presented below was largely written by User:NordNordWest and signed by almost 120 people involved in German Wikimedia projects. It highlights the many concerns and worries of the German-speaking community, so we believe it can enhance the discussion on these issues. We would like to thank everyone involved.

This text was published in German simultaneously in the Wikimedia Deutschland-blog and in the Kurier, an analogue to the English "Signpost". This translation has been additionally placed on the talkpage of the WMF-privacy-policy-draft at Meta.

(preface Denis Barthel (WMDE) (talk), 20.12.)

Starting position

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. On the one hand, a diverse range of security features are available to registered users:

- Users can register under a pseudonym.
- The IP address of registered users is not shown. Only users with CheckUser permission can see IP addresses.
- Users have a right to anonymity. This includes all types of personal data: names, age, background, gender, family status, occupation, level of education, religion, political views, sexual orientation, etc.
- As a direct reaction to Snowden's revelations, the HTTPS protocol has been used as standard since summer 2013 (see m:HTTPS), so that, among other things, it should no longer be visible from outside which pages are called up by which users and what information is sent by a user.

On the other hand, however, all of a user's contributions are recorded with exact timestamps. Access to this data is available to everyone and allows the creation of user profiles. While the tools were running on the Toolserver, user profiles could only be created from aggregated data with the consent of the user concerned (opt-in procedure). This was because the Toolserver was operated by Wikimedia Deutschland and therefore subject to German data protection law, one of the strictest in the world. However, evaluation tools that were independent of the Foundation and any of its chapters already existed.

One example is Wikichecker, which, however, only concerns English-language Wikipedia. The migration of programs to ToolLabs, which means that they no longer have to function in accordance with German data protection law, prompted a survey of whether a voluntary opt-in system should still be mandatory for

XI's Edit Counter or whether opt-in should be abandoned altogether. The survey resulted in a majority of 259 votes for keeping opt-in, with 26 users voting for replacing it with an opt-out solution and 195 in favor of removing it completely. As a direct reaction to these results, a new tool – Deep User Inspector – was programmed to provide aggregated user data across projects without giving users a chance to object. Alongside basic numbers of contributions, the tool also provides statistics on, for example, the times on weekdays when a user was active, lists of voting behavior, or a map showing the location of subjects on which the user has edited articles. This aggregation of data allows simple inferences to be made about each individual user. A cluster of edits on articles relating to a certain region, for example, makes it possible to deduce where the user most probably lives.

Problems

Every user knows that user data is recorded every time something is edited. However, there is a significant difference between a single data set and the aggregated presentation of this data. Aggregated data means that the user's right to anonymity can be reduced, or, in the worst case, lost altogether. Here are some examples:

- A list of the times that a user edits often allows a deduction to be made as to the time zone where he or she lives.
- From the coordinates of articles that a user has edited, it is generally possible to determine the user's location even more precisely. It would be rare for people to solely edit area X, when in fact they came from area Y.
- The most precise deductions can be made by analyzing the coordinates of a photo location, as it stands to reason that the user must have been physically present to take the photo.
- Places of origin and photo locations can reveal information on the user's means of transport (e.g. whether someone owns a car), as well as on his or her routes and times of travel. This makes it possible to create movement profiles on users who upload a large number of photos.
- Time analyses of certain days of the year allow inferences to be drawn about a user's family status. It is probable, for example, that those who tend not to edit during the school holidays are students, parents or teachers.
- Assumptions on religious orientation can also be made if a user tends not to edit on particular religious holidays.
- Foreign photo locations either reveal information about a user's holiday destination, and therefore perhaps disclose something about his or her financial situation, or suggest that the user is a photographer.
- If users work in a country or a company where editing is prohibited during working hours, they are particularly vulnerable if the recorded time reveals that they have been editing during these hours. In the worst-case scenario, somebody who wishes to harm the user and knows extra information about his or her life (which is not unusual if someone has been an editor for several years) could pass this information on to the user's employer. Disputes within Wikipedia would thus be carried over into real life.

Suggestions

Wikipedia is the fifth most visited website in the world. The way it treats its users therefore serves as an important example to others. It would be illogical and ridiculous to increase user protection on the one

hand but, on the other hand, to allow users' right to anonymity to be eroded. The most important asset that Wikipedia, Commons and other projects have is their users. They create the content that has ensured these projects' success. But users are not content, and we should make sure that we protect them. The Wikimedia Foundation should commit to making the protection of its registered users a higher priority and should take the necessary steps to achieve this. Similarly to the regulations for the Toolserver, it should first require an opt-in for all the tools on its own servers that compile detailed aggregations of user data. Users could do this via their personal settings, for example. Since Wikipedia was founded in 2001, the project has grown without any urgent need for these kinds of tools, and at present there seems to be no reason why this should change in the future. By creating free content, the community enables Wikimedia to collect the donations needed to run WikiLabs. That this should lead to users losing their right of anonymity, although the majority opposes this, is absurd. To ensure that user data are not evaluated on non-Wikimedia servers, the Foundation is asked to take the following steps:

- Wikipedia dumps should no longer contain any detailed user information. The license only requires the name of the author and not the time or the day when they edited.
- There should only be limited access to user data on the API.
- It might be worth considering whether or not it is necessary or consistent with project targets to store and display the IP addresses of registered users (if they are stored), as well as precise timestamps that are accurate to the minute of all their actions. The time limit here could be how long it reasonably takes CheckUsers to make a query. After all, data that are not available cannot be misused for other purposes.

submitted by [Silke WMDE](#) (talk) 16:21, 20 December 2013 (UTC)

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 13



WIKIMEDIA
META-WIKI

- Main page
- Wikimedia News
- Translations
- Recent changes
- Random page
- Help
- Babel

Community

- Wikimedia Resource Center
- Wikimedia Forum
- Mailing lists
- Requests
- Babylon
- Reports
- Research
- Planet Wikimedia

Beyond the Web

- Meet Wikimedians
- Events
- Movement affiliates
- Donate

Print/export

- Create a book
- Download as PDF
- Printable version

Tools

- What links here
- Related changes
- Special pages
- Permanent link
- Page information
- Link by ID

Content page Discussion Read Edit Add topic View history

Search Meta Go

Talk:PRISM

The following discussion is closed. Please do not modify it. Subsequent comments should be made in a new section. A summary of the conclusions reached follows.

Based on the discussion below, the WMF legal team feels that there is general support for some PRISM-related action. However, we feel that the current proposals are either not strongly supported, or there are genuine concerns or reservations about them. The team will therefore continue to monitor the situation. In particular, in keeping with the consultation below, we will look for opportunities for action and collaboration that are:

- Focused on the movement's mission and values - for example, actions focused on ensuring reader privacy, or on protecting WMF's right to be transparent with the community
- Consistent with our international nature - in other words, actions that do not not privilege one country's citizens over another

We also recognize the questions and concerns raised here about privacy, and urge interested community members to continue that discussion as part of our larger privacy policy call for input.

Thanks to everyone who participated in the consultation. We encourage further discussion, including suggestion of potential actions, either through the new section at the end of this page, or through the advocacy-advisors list.

LVilla (WMF) (talk) 21:34, 11 July 2013 (UTC)

Contents [hide]

- 1 What wasn't said
- 2 Better supporting anonymous contributions
- 3 What types of logs does the Wikimedia Foundation keep, for how long and in what level of detail?
- 4 Thirty day rule?
- 5 June 21
- 6 Community Feedback
- 7 On establishing servers in other countries
- 8 Should we join with these organizations in their public statements and efforts as they relate to the Wikimedia community's values and mission?
 - 8.1 Update
- 9 Stop logging IP addresses
- 10 "law-enforcement agency or a court or equivalent government body"
- 11 A U.S. issue?

- 12 Comments copied from Blog
- 13 PRISM concerns Trust, Trust concerns Wikipedia
- 14 Snowden as Wikimania's keynote speaker
- 15 Historical Background
- 16 Call for input on WMF privacy policy
- 17 Universal Declaration of Human Rights
- 18 and now?
- 19 PRISM is not everything
- 20 Wikimedia may be lying
- 21 Further feedback and suggestions
 - 21.1 Copied from above
 - 21.2 Followup blog post
- 22 We should sign the global Principles on Surveillance guidelines
- 23 Meu temor(como brasileiro):

What wasn't said [edit]

This statement appears to carefully avoid speaking to the ongoing surveillance and traffic interception which Wikimedia has specific knowledge of but which itself is not actually an active party to, I think this is unfortunate and misleading.

I also note that the claims that Wikimedia has 'not "changed" our systems to make government surveillance easier' is, in my well informed opinion, basically a lie by omission: By failing to move all reader traffic to SSL wikimedia has failed to change its systems in order to limit the ongoing traffic observation and manipulation which it is specifically aware of (and, generally, to also protect against additional surveillance which Wikimedia may not be aware of). Because the traffic is unencrypted there would be little reason for any government to seek out Wikimedia's cooperation. With no active involvement required Wikimedia would have no opportunity to oppose blanket surveillance in a court of law. Evening ignoring the fact that Wikimedia is already aware that its traffic is being intercepted the use of SSL is a best practice which is already employed by default for all users on many popular websites.

It is my personal experience that in the past Wikimedia has not considered the privacy of its readers to be a high priority. I have never quite been able to understand why: My view has always been that to many people Wikipedia is an extension of their mind and their access patterns betray some of their most personal and intimate thoughts. But whatever the reason, adopting best practices to protect reader privacy has simply not been a priority and I've accepted that although I did not agree with it. But now I'm confused with the manner in which this post fails to acknowledge this past indifference while simultaneously claiming to care deeply. I would be delighted to hear that there was a change in priorities here, but considering the history it seems like this is simply a politically expedient response to a fad issue which will soon be forgotten. --Gmaxwell (talk) 00:45, 15 June 2013 (UTC)

This certainly seems like a fad issue. While I'm not sure I'd characterize the lack of forced SSL in the same way you do, I think working on documents such as User:Sue Gardner/Wikimedia Foundation Guiding Principles is a much better use of time and other resources. This allows us to define what we stand for and what we believe, rather than

simply denouncing whatever the latest government abuse (or potential future abuse) happens to be in the news at the moment (SOPA, PRISM, etc.).

For what it's worth, bugzilla:47832 is the relevant bug about enabling HTTPS for all users. I doubt we'll see this happen this year or next, though.

And, at some level, there is a reasonable argument that some level of user responsibility is warranted. That is, stable HTTPS access (using pretty URLs) is currently available to anyone interested in using it. –MZMcBride (talk) 04:01, 15 June 2013 (UTC)

well ssl is important, and I wish it was on all the time, i don't think it quite provides the protection you think it does. People can still do fingerprinting based on size of things requested. If you edit, the exact timestamp is recorded, which if the government is monitoring all the inbound ssl traffic should be enough to match you up to who you are. (Ssl only protects the content of the message. Not who sent it or that a message was sent. In the context of wikimedia where the message is already known or is public (usually), this isnt a lot of protection. (The biggest benefit in our context is protection against shared session attacks).Bawolff (talk) 15:27, 15 June 2013 (UTC)

SSL or TLS ? Which versions are supported, which one are deprecated and its support should be removed ? verdy_p (talk) 16:33, 15 June 2013 (UTC)

Well this conversation is talking about encrypting http in general. Which version of SSL/TLS and if it is secure, is an implementation detail (An important implementation detail no doubt, but still off topic). Wikipedia apparently supports SSL3 and TLS1.0 according to <https://www.ssllabs.com/ssltest/analyze.html?d=en.wikipedia.org> Bawolff (talk) 19:07, 15 June 2013 (UTC)

Hello Greg, can you say more about this surveillance and interception? Are you talking about datacenter-level or backbone-level surveillance?

And yes, let's finish enabling HTTPS by default for everyone. I don't see anyone suggesting obstacles to making that happen, other the observation that it hasn't happened yet. The comments on the relevant bugs seem to be ideas or positive reactions. And speeding the transition to SSL-only service is one effective way we can swiftly increase reader privacy, regardless of what is in our public statements of principle. –SJ talk 23:48, 15 June 2013 (UTC)

Even having https by default it would not be efficient for most of people: if users use a navigator which collect data. In this case, the software send statistics with "listening" on the input and output data, even with a SSL layer. Information are sent encrypted to the developer company. I especially think to google chrome and it's HTTPs everywhere feature: "Nobody" can sniff data; except google. It is probaly the same with IE; safari etc... It is possible to think that they can send passwords if the user choose to record them

The use of some add-on can create the same problem.

Some Os (especially mobile one) send data by simply check-in a developer company server. I think to android which do things like time tracking per application. This make difficult to understand why nobody tried to create a build with stat funtion removed from android source code. Apple doesn't seems to collect data with OSx. It dosen't prevent to do this with

So instoring encryption by default aiming at spying programs would only have the effect to slow down connection with SSL headers, most of the time. It is useless until users of such software or OS recieve a warning banner. 2A02:8422:1191:6E00:56E6:FCFF:FEDB:2BBA 01:02, 16 June 2013 (UTC)

- **Comment** SSL is good for concealing stuff like passwords, but it's of no help for keeping private what articles people are reading, since the message lengths are usually enough to identify articles even if the packets are encrypted. Adding some random padding to each message before encryption can fuzz this up a little bit, but not enough to matter. Also, Firefox 20 (I haven't tested other browsers) sends an OCSP request to Digicert (iirc) whenever you view an article on the secure site. That means Digicert gets the IP address of everyone who reads Wikipedia through SSL, which doesn't seem so great, although OCSP in general is a good idea. 50.0.136.106 07:21, 20 June 2013 (UTC)

The OCSP request is not very helpful to determine what you are reading. In fact, since we have now SUL activated by default, the secure connection can be proxied from a random site owned by the WMF, and unrelated to the wiki you are actually reading (that secure proxy can then be used to visit all Wikimedia sites, and for a limited time, it could be used to navigate to other sites, within a secure frame, and for a limited set of protocols, only HTTP sites; to vicite external HTTPS sites, the proxy will not be used, that proxy will cache these external visits in a Squid server, for a limited time : one hour max, isolating the sessions as much as possible, but this proxy won't support external cookies very well, except temporary session cookies so this may limit the interactions with these external sites).

For the user's browser, all will appear as if they were visiting the randomized proxy as the main site, and the HTTPS session will appear being originating from of a visit of this WMF proxying site. Digicert won't be able to determine which Wikimedia project you're actually visiting with HTTPS connected to that random proxy (With SUL, the session is identified and communicated to other actual projects using internal security tokens, and a single session is established for all wikis. In fact the proxies are located directly on the existing farm of Squid servers for any WMF project. verdy_p (talk) 23:47, 20 June 2013 (UTC)

- **Comment** Why not making wkimedia domains available with the .onion extension in more than SSL. It would be a message that this extension is not only used by bandits. 2A02:8422:1191:6E00:56E6:FCFF:FEDB:2BBA 13:20, 3 July 2013 (UTC)

Better supporting anonymous contributions [edit]

I repeat my comment: SSL or TLS ? And this is NOT off-topic, because you always use **SSL** when in fact you should speak about **HTTPS**.

SSL is deprecated (and too much unsecure if we think about what developers PRISM can do) ! What I mean is that the level of security needed in HTTPS and supported by Wikimedia sites should be specified. The strongest algorithms should be used, and users should be warned if their connection configuration do not support it. Otherwise they will

Yes, falsey protected if they just see "https" or the security icon in their address bar or status bar !

In other words, **Wikimedia sites should display the current security level of their connection. It should also allow evaluating the security of their local account** (user password, inspection of the email confirmation : users can copy-paste the MIME headers of the confirmation email they recieved, or the MIME headers of the last mail sent to Wikimedia for posting images, or the informations added in HTTP headers by some browser plugins, or inspection of their version and known defects, suggesting upgrades or removal of these unsecure plugins), even before they create a local account, or when creating it by evaluating the strength of their password, because the local account will be the only protection they'll have for their pricay, by hiding to others their connection IP. If an account is stolen or spied (by an intruder that broke the security algorithms), it should still not allow inspecting the connection history. And may be it should even hide to users the email address that they have registered, by encrypting it once the email has been confirmed (the only thing that a user will be able to do is to change the email address, or reconfirming what they think is their own address).

All registered users should be notified immediately at their old email address to confirm the change of email address (to avoid it to be replaced by another proxying and spying email address). As the email address will now be invisible in the user's preferences to the user as well as to any possible spier, it will be impossible to know who really owns that account (this should be kept by Wikimedia sites in a secure database (so all subscribed notifications will be sent to an address that no spier should know).

And Wikimedia should also monitor the security of its mailservers for its outgoing emails going to the email address of a registered user (this means securing its DNS server, asserting the DNS entries, using all possible antispoofind technics, verifying mail server secure signatures...), because these emails are the main tool by which a user could still be identified, even if they are IP-connected via an anonymizing proxy.

But of course, users that want to communicate with Wikimedia sites on *politically sensitive subjects*, should avoid revealing their own identity online in their talk pages or when discussing in any public spaces or on talk pages of other users.

Instead, they should create a new specific (and unrelated) account for these activities, using an alternate email for registering it. Then they should use tools offered in their User's preferences page to assert the security of this new account.

Another idea:

If users fear their account on Wikimedia has been compromised, they should immediately ask the deletion of this registered account, for possibly creating a new one (the contributions will be kept, but will be anonymized using a user name like "anonymous-`<random-hexadecimal-id>`" in the history, the old account will be locked and no longer accessible to anyone.

All users should be offered an oppotunity to create an "**publicly anonymous secondary account**" : if they have one, and make any contribution on Wikimedia using their normal non-anonymous account, then Wikimedia should ask them if they intended to use the anonymous account instead: they can confirm it each time or instruct Wikimedia to stop

asking for the next hour. If they want to use the secondary account, Wikimedia will present them a secure logon screen asking for the secondary password. As this account is anonymous, it should not need to be working under SUL (each wiki will use its own local database of anonymous user accounts). Once they are connected to the two accounts, two icons are shown at top of page: their regular user name, and the "anonymous" account name, they can click on one of them to select which one to use (if they use the anonymous account, Wikimedia will not ask them to confirm their edits. If the anonymous session is idle for more than one hour, it will be automatically logged out (the session cookie should not last for more than one hour), and the anonymous icon will be shown in its disconnected state, even if they are still connected on their regular account (and Wikimedia will restart asking them if they want to use their anonymous account for their edits).

The secondary anonymous account may inherit immediately, at creation time, of some privileges from the primary regular account (notably the autoconfirmed status, but NOT any admin privileges). Users may also opt for creating an anonymous account directly, without any associated regular account (but then they'll start with no privileges, like all other newly registered regular users): in fact this should be the best solution for supporting anonymous users, we should encourage them to do so, instead of using their IP-only connection, logged in public histories (they can still register their email with it, and be sure that they'll be able to reuse this same account on later connections): even if they are logged on, these anonymous users with a personal account should be kept logged on for a maximum of 1-hour of idle time (regular accounts may continue staying connected for 1 month). And even if they only have an anonymous account, they can also be offered the option to create a primary regular account, like other users (for their non-sensitive editing or reading sessions; in that case Wikimedia will also ask them every hour if they should not use their existing anonymous account when accessing one page). Some pages should also not be warned by Wikimedia: the anonymous account may specify a list of pages, or categories, or namespaces, where Wikimedia will not ask them if they wish to use their anonymous account instead.

Registered anonymous users should also be allowed to participate to secured community polls (they will be able to vote only once), if this account is associated with a regular account (the vote will be visible to others as coming from a registered anonymous account, but then they won't be able to vote with their regular account as well). The secure vote server will check internally the status of the anonymous account, and will be able to see if the regular account has already participated or if another past anonymous account has voted (if so, users won't be able to vote again or will or change their vote, unless they ask to Wikimedia server to delete their old anonymous vote; this vote deletion will be performed securely).

Only one active (undeleted) anonymous account may be associated at any time to a regular account (this will limit abuses, notably with spammers, even if the CheckUser admin team may see with which regular account the anonymous account is associated. Some abusers may also be restricted (by spamfighters) from using their anonymous account for some time and informed. This event may be logged in their regular account that they may continue to use).

This will also be useful when contributing in some subjects with a regular account, when there are personal conflicts (this could calm others, avoiding personal wars or personal defamation).

The list of past (deleted) anonymous accounts, as well as the current active anonymous account will be kept in the regular user account history, for a limited time, only to help fighting spammers; this should not exceed 1 month).

Creating and activating a publicly anonymous account should be a two click action (including for generating the password: users need to copy the generated string password, because it will later be encrypted and never shown again to anyone (including the user), but the user can request the deletion of this account and creation of a new one with a newly generated password (overridable by the user typing a password of his choice and confirming it).

Even for regular (publicly non-anonymous) registered accounts, this should be simple, and Wikimedia should immediately propose a strong password before the user overrides it. All accounts (anonymous and non-anonymous, should have a one-click button in their preference page, to generate a new string password and fill the two input boxes where they can change and confirm it (when the user types his own password, it is hidden by default, when the user clicks the "generate strong password", it will be shown and stay on screen, it will be used only if the user accepts it by confirming the preferences; but for accessibility reasons, there should still be a checkbox to hide/show the content of the password input and password confirmation box). verdy_p (talk) 23:29, 20 June 2013 (UTC)

What types of logs does the Wikimedia Foundation keep, for how long and in what level of detail? [edit]

Before we can start to consider actions by the Foundation, I think it's appropriate for us to look at our own logs and how PRISM could affect us. There was a thread brought up on Wikimedia-l about this topic this week. I didn't have a chance to read it fully but from a brief skim of it, I believe it's unclear exactly what information the Foundation keeps, and for how long. There was a link to a mailing list post by Domas from 2010 saying it's a 1/1000 sample, but other comments referred to a full access log for the past 30 days. Therefore, please can we get the relevant technical details from **all** teams with access to logs of what data is stored and for how long? I don't know the full details, but a few ideas would include asking the Analytics team (who use the new Kraken machine), whoever is using the raw data to produce <http://reportcard.wmflabs.org/>, general reader access logs, error logs etc.

Thehelpfulone 00:28, 15 June 2013 (UTC)

Yes please. We should assume any record we keep might be accessed one day so the best preparation for this is to minimise the records we keep. If we don't have them then they can't be accessed. Filceolaire (talk) 00:43, 15 June 2013 (UTC)

- Well, these are the things we know they have per browser operation and Help:CheckUser#Information returned; article accessed, date/time of access, referer, username, IP address, user agent (browser, operating system, blah, blah, blah) and XFF headers. Depending on who you talk to, this info is supposedly purged after 30, 60 or 90

days. But it has been acknowledged that some of this information is copied to the checkuser wiki, arb wiki, etc. where it is kept permanently. 64.40.54.96 05:35, 15 June 2013 (UTC)

This shouldn't be a "depending on who you talk to" situation. We're pretty open about it - the data is purged after 90 days. Data on long-term abusers *may* be copied to the Checkuser wiki for later use in analysis to determine whether future vandalism is related to a long term abuser, but that's incredibly rare, when viewed as a percentage of the whole. Philippe (WMF) (talk) 07:53, 15 June 2013 (UTC)

I think the original comment was about access logs for readers, not authors who edit. For how long is the access log kept for readers and is there an access log for all readers or just a 1/1000 sample? --Tobias talk · contrib 08:00, 15 June 2013 (UTC)

I have no idea. Deferring to those who know. :) Philippe (WMF) (talk) 09:55, 15 June 2013 (UTC)

I second that question. A EU citizen myself, and even though Wikimedia might not own or borrow servers in the European Union, how close are the Wikimedia servers from the requirements of the EU law ? It was alleged here, in 2011 [#] that *EU legislation, (...) requires search engines to purge all data relating to end users after a six month period.*

User:Philippe (WMF) says above : "data is purged after 90 days". I am afraid that as long as this is not clearly written in http://wikimediafoundation.org/wiki/Privacy_policy [#], there is no guarantee that the Wikimedia Foundation is intending to enforce this kind of regulation and serious about it. Is there anything that can guarantee that the Wikimedia Foundation cannot change the present "90 days" of today into "90 years" tomorrow without warning and consultation with the community and sufficient warning of the end user as regards the "terms and conditions" ? Teofilo (talk) 18:49, 15 June 2013 (UTC)
Agreed: this should be part of our privacy policy. --SJ talk 23:48, 15 June 2013 (UTC)

I had always had the impression that logs of editing operations were kept around for a while, but access logs were not--and in particular that CU couldn't tell what articles people were reading. If they can, I find that scary and invasive, but potentially useful in sock investigations. I would urge getting rid of all logging of read-only accesses, including aggregated logging such as viewcounts on articles and geolocations. There could be some very limited exceptions for dealing with ops problems (DDOS origins, etc) but any such info (about human readers, I'm less concerned about automated clients especially malicious oens) should never be disclosed. 50.0.136.106 07:28, 21 June 2013 (UTC)

Thirty day rule? ^[edit]

I thought there was some thirty day rule comment period related to proposals of this nature. Maybe I'm thinking of something else.

I suppose the Wikimedia Foundation could sign, but that wouldn't necessarily be representative of Wikimedia signing. --MZMcBride (talk) 00:55, 15 June 2013 (UTC)

I assume you're talking about these policies? It doesn't look like there is a deadline (both a 'if times permits' clause to allow exceptions and no actual expectation of a deadline

(UTC)

MZMcBride, that was for changes to the terms of use, I think. I'm not sure if the privacy policy is a subset of the terms of use, or if it's a separate contract. -

-NaBUru38 (talk) 20:21, 18 June 2013 (UTC)

June 21 [edit]

What happens on June 21 that makes that day the final day of community consultations? Don't you think that it's at least eyebrow-raising that it took the WMF 8 days (since the news first broke out on June 6) to write a blog post, and you only give the community 7 days to comment on it? How are you planning to get the wider community to comment on this? Are there any plans for CentralNotice/Watchlist campaigns asking people to comment, or are you perhaps planning to use EdwardsBot to send a notice to the village pumps? odder (talk) 00:57, 15 June 2013 (UTC)

Hi, Odder - the blog post came out today, but we asked for comment on wikimedia-l and advocacy-advisors on June 11th (and have been following the conversation on both of those lists). That said, if the community thinks the correct answer is "take more time" we're open to that too; our main interest in speed is because the earlier we move, the greater the opportunity to actually impact the discussion. - LVilla (WMF) (talk) 01:59, 15 June 2013 (UTC)

Thanks for the explanation, Luis—I was mostly afraid that 7 days might not be enough time for the wider Wikimedia community to comment on this proposal. Your answer clears this up, so thanks again. odder (talk) 13:47, 15 June 2013 (UTC)

Community Feedback [edit]

"It's important for Wikimedia to be a voice of opinion in these matters, but joining a group to back the opposition of PRISM doesn't seem like the most successful avenue to me. I think whenever an association is made with another organization or group of organizations it is easier for the whole group to find itself with potential liability. One company can never be completely sure of another company's origin, path and trajectory - take Invisible Children as an example - and the risk of being jointly discredited for something possibly inconsequential could affect the momentum of the movement at large. I think that many organizations taking individual stances on the issue weighs heavier than a conglomerate doing the same."

—Glenn Sorrentino ✉

Hi, Glenn- Many of the organizations behind stopwatching.us have extremely long track records of doing the right thing: EFF, FSF, and CDT have all been doing rights advocacy for around 20 years, and while Mozilla is relatively new to direct activism, it also has a long track record of having strong values like ours. That said, if you feel we should have a voice, just not through stopwatching.us, what other suggestions would you make about how we should advance our views? — LVilla (WMF) (talk) 16:11, 15 June 2013 (UTC)

Some might have a "long track record of doing the right thing" but some of their fellow

servers are, shall we say, controversial. Snowden was photographed with an EFF sticker on his laptop, suggesting he supports these "strong values." Yet Snowden's particular version of what he presumably considers to be "strong values" led him to seek employment with his latest employer with the advance purpose of getting access to secrets that he could then reveal without authorization. This is controversial, to say the least. If it wasn't controversial, surely a country with a better track record on Internet freedom than China or Russia would be sheltering him. I am amazed at how the WMF keeps finding the bad guys in the form of large numbers of U.S. Congressmen as opposed to somewhere else (first with SOPA/PIPA and now with PRISM which Congress has long been aware of).--Brian Dell (talk) 17:29, 25 June 2013 (UTC)

On establishing servers in other countries [edit]

At Meta:Babel#Wikimedia_servers_and_NSA_wiretapping I started a discussion on the possibility of the foundation establishing other servers in other countries partly so individual connections are less likely to be wiretapped.

Please read Stefan2's comments on that page.

So far Wikimedia has servers in Tampa, FL, Ashburn, VA, and Amsterdam. Considering that data usually takes the cheapest route rather than the most direct, where else should the foundation get servers? We have to take in consideration money that the WMF has and the political inclinations of the countries where the new Wikimedia servers are set up. For specific locations, would anyone like to evaluate the following locations? Singapore, Hong Kong, Brazil, South Africa... and I am not sure if the political climate in Dubai would support a WMF server there.

The idea is that, say, if an individual in Pakistan wants to connect to Wikimedia projects, he/she can connect to servers in Dubai, or if a person in Malaysia wants to connect, he/she can connect to servers in Singapore.

WhisperToMe (talk) 04:27, 15 June 2013 (UTC)

I'm not an expert on this, but it seems to me that increasing the potential number of jurisdictions that servers live in actually increases the risk of wiretapping, not decreases it, right? I mean, any of those countries could order a wiretap on a server, and all of a sudden we're up from one potential governmental player to several. Philippe (WMF) (talk) 07:57, 15 June 2013 (UTC)

We have a server in the Netherlands, so that's two government players so far.

WhisperToMe (talk) 14:38, 15 June 2013 (UTC)

{{citation needed}}, please. odder (talk) 16:12, 15 June 2013 (UTC)

Wikimedia servers#Hosting says "As of June 2010, we have four colocation facilities:" with two in Tampa and two in the Netherlands, and "As of 2012 there are also servers in Ashburn, Virginia (eqiad)" WhisperToMe (talk) 17:11, 15 June 2013 (UTC)

You wrote we had a *server* in the Netherlands, which is not true.

Additionally, I would also suggest that you check what are the roles of the

NL servers before jumping to any conclusions. User (talk) 17:16, 15 June 2013 (UTC)

Okay, so I should have said two servers or one location. Nonetheless the point was that we also have facilities in the Netherlands. Anyway I followed the link to "Server roles" on Wikitech from the Wikimedia servers#Hosting page, and the page is blank. However I found wikitech:Category:Servers (should I redirect "Server roles" to that page?). Each of those pages don't have information on geographical locations, but I found wikitech:Amsterdam cluster WhisperToMe (talk) 17:24, 15 June 2013 (UTC)

Doing further digging the Amsterdam cluster is a part of wikitech:Category:Esams cluster. I'm going to file through wikitech:Category:Clusters to get a count of geographical locations. WhisperToMe (talk) 17:30, 15 June 2013 (UTC)

Aside from the Esams cluster: wikitech:Category:Eqiad cluster -> Ashburn, VA. wikitech:Category:Knams cluster -> wikitech:Kennisset cluster (Amsterdam). Lopar cluster seems to be in (Tampa) Florida (wikitech:Lopar cluster mentions caching out of Florida). Pmtpa cluster -> Tampa, Florida (wikitech:Tampa cluster). The page on the Ulsfo cluster (wikitech:Ulsfo) is blank. WhisperToMe (talk) 17:34, 15 June 2013 (UTC)

Okay, I found a page on the network design: Wikitech:Network design - It goes over the US network and the European network WhisperToMe (talk) 17:41, 15 June 2013 (UTC)

Notes some of the pages at wikitech are rather outdated. (For example, Isn't lopar long gone?). Perhaps looking through the lists of server types at ganglia would give you a better idea. My understanding [**which could be wrong**. Don't trust me. I do not know what I'm talking about] is that most of the "real" servers are in US, with esams (netherlands) having squid/varnish caching servers, that just forwards requests (other then anons who aren't editing) to the backend servers in VaginaVirginia [Bad auto-spelling correct]. Bawloff (talk) 18:10, 15 June 2013 (UTC)

You mean Virginia, right? :) WhisperToMe (talk) 18:29, 15 June 2013 (UTC)

For our readers having multiple countries with servers may give some comfort, especially if there was some way to choose which server to connect to. I'm not convinced things work so well for editors, if you have more than one copy of a database open for editing you will get synchronisation issues. WereSpielChequers (talk) 14:56, 15 June 2013 (UTC)

That's a good point. Who are the WMF board members or officials who know the most about this? Based on the PRISM charts it may mean that Latin America & Caribbean and the Asia Pacific Regions may be the best place to establish Wikimedia

servers (it seems like those in Africa can connect to European servers). So I think the WMF should study Hong Kong, Singapore, Brazil, and/or Panama (or another Central American country which can be neutral) as ideas for server locations. WhisperToMe (talk) 15:32, 15 June 2013 (UTC)

It is useless, according to the end of this film about the NSA wiretrapping program (NSA - L'agence de l'Ombre) (author: James Bamford and C Scott Willis) (2008), the NSA is also watching all strategic point of internet across the world, with subprograms affiliated indirectly to PRISM. So it is not limited to the US. 2A02:8422:1191:6E00:56E6:FCFF:FEDB:2BBA 21:40, 15 June 2013 (UTC)

Does the film say where these end points are? WhisperToMe (talk) 00:17, 16 June 2013 (UTC)

No, they don't list all of them. The film say there are satellite communication sniffing. I can also say that certain under sea cable landing have optical splitters. The film give only details (to show an example) about Moro Bay in California: It give a full explanation about where the data is collected. You can find some part of the example at cryptome , but you won't understand many things with this web page.

The film is based on a book : The Shadow Factory: The NSA from 9/11 to the Eavesdropping on America.

You have a lot of more information on those parts with the film rather than the PRISM leaks.

The original language is in english, but as I saw the film on the TV, all was translated, including the title. I can't find the original one.

2A02:8422:1191:6E00:56E6:FCFF:FEDB:2BBA 03:10, 16 June 2013 (UTC)

Thank you for the info! I'm going to try to find this book and get as much information about NSA wiretapping locations (now we will assume whatever Bamford says is true) as possible and perhaps the WMF can find information on how best to avoid this wiretapping. Locations for new WMF servers can be based on this information. Also it may be good to have backup servers in "neutral" countries in case the possibility of war comes. I would hate to see all of our hard work wiped out. I have been working on Wikimedia projects for almost ten years, so I'm sure you understand how I feel about this. WhisperToMe (talk) 02:56, 17 June 2013 (UTC)

2A02:8422:1191:6E00:56E6:FCFF:FEDB:2BBA: I saw a video on YouTube which seems to be what you watched.

- Bamford's message was routed from en:Kuala Lumpur, to en:Mersing, Malaysia where it entered an undersea cable along the South China Sea to through en:Shantou, China, and then in an undersea cable to an area near en:Morro Bay, California, to a building near en:San Luis Obispo (80% of all communications from Asia to the US enter through this building, but under new NSA orders they don't tap in here), and then to the AT&T Regional Switching Center in en:San Francisco (this is where the NSA taps into the connection) -- So, if I am correct, if the reader traffic in East/Southeast Asia goes to Singapore or Hong Kong and it doesn't go via satellite, it will avoid

I'll check if the NSA book has more information

WhisperToMe (talk) 06:10, 17 June 2013 (UTC)

I won't have a static ip this week. If you want to know which routers is used by a request, I suggest you the **tracpath6(article)** command. tracpath give you generally more details (more hops) than traceroute. Here is an example of a traceroute6 result from Dalas:

```

hop      rtt      rtt      rtt      ip address      fully
qualified domain name
1        7        7        6        2001:470:1f0e:513::1
hexillion-2.tunnel.tserv8.dall.ipv6.he.net
2        8        1        1        2001:470:0:78::1      gige-g2-
14.core1.dall.he.net
3        29       25       24       2001:470:0:1b6::2
10gigabitethernet5-4.core1.atl1.he.net
4        33       41       34       2001:470:0:1b5::1
10gigabitethernet16-5.core1.ash1.he.net
5        39       38       58       2001:470:0:299::2
100gigabitethernet7-1.core1.nyc4.he.net
6        108      107      116      2001:470:0:128::2
10gigabitethernet1-2.core1.lon1.he.net
7        118      115      138      2001:470:0:3f::21
10gigabitethernet1-1.core1.ams1.he.net
8        117      117      117      2001:7f8:1::a504:8539:1
9        120      125      124      2a00:d10:1144:61::468
vlan61.br.en1.oxilion.net
10       121      121      121      2a00:d10:1144:62::731
vlan62.n5k-a.en1.oxilion.net
11       116      116      116      2a00:d10:101::11:1
ergens.org

```

```

dal=Dallas
atl=Atlas
I don't know for ash
nyc=New York City
lon=London
ams=Amsterdam

```

If you want a good answer for server location: The best place for data center is everywhere in the world.

Let me explain: There is a technique originally created to reduce load on the public network. Instead of creating a big server in one place (wikmedia use also separate servers in Europe), you choose to have "medium" data centers divided all over the world. Each place contain a copy of the whole webs sites. With a same host name, the list of ip address you get will varies according to servers workload and your geographic location.

This technique of geographical web placement has a name, which I forgot and probably a wikipedia article. It is used by big firms like Google. You can make the test on companies like these: If you launch a tracepath, the number hops will be always fewer than most sites, and independently from the place you are located.

2A02:8422:1191:6E00:56E6:FCFF:FEDB:2BBA 02:19, 18 June 2013 (UTC)

I'm in the US myself, but this would be fun to try! According to your vision, do you have cities in mind which would be good places for these medium data servers? How many such medium servers would you establish per continent? WhisperToMe (talk) 05:27, 18 June 2013 (UTC)

Sorry, I've been busy since last time. I'm afraid that I don't have a real answer. This is just something I learned when I was studying DNS. I know google have serveral location in europe, but if I do a host on yahoo...

```
root@sysresccd /root % host www.yahoo.com
www.yahoo.com is an alias for fd-fp3.wg1.b.yahoo.com.
fd-fp3.wg1.b.yahoo.com is an alias for ds-fp3.wg1.b.yahoo.com.
ds-fp3.wg1.b.yahoo.com is an alias for ds-eu-fp3-
lfb.wal.b.yahoo.com.
ds-eu-fp3-lfb.wal.b.yahoo.com is an alias for ds-eu-
fp3.wal.b.yahoo.com.
ds-eu-fp3.wal.b.yahoo.com has address 87.248.112.181
ds-eu-fp3.wal.b.yahoo.com has address 87.248.122.122
ds-eu-fp3.wal.b.yahoo.com has IPv6 address
2a00:1288:f00e:1fe::3000
ds-eu-fp3.wal.b.yahoo.com has IPv6 address
2a00:1288:f00e:1fe::3001
ds-eu-fp3.wal.b.yahoo.com has IPv6 address
2a00:1288:f006:1fe::3001
ds-eu-fp3.wal.b.yahoo.com has IPv6 address
2a00:1288:f006:1fe::3000
```

there are alias which contains eu. It make think yahoo have only one point for the whole european union. You probably won't have the same density in south corea as in Sahara. I must say that I know absolutely nothing about the synchronisation thecniques that are used, and i don't really know sor dns too.

With the high number of law voted in US & eu for allowing thing this, I don't understand why peoples warm only now. If you think to the number of contries where drones work. You can realize most of peoples are safe.

For the rest of the world the main risk is unemployment, but it is not linked to any government. 2A02:8422:1191:6E00:56E6:FCFF:FEDB:2BBA 14:08, 3 July 2013 (UTC)

Should we join with these organizations in their public statements and efforts as they relate to the Wikimedia community's values and mission? [edit]

- +1 --Isderion (talk) 13:54, 15 June 2013 (UTC)
- Should Wikimedia join in decrying PRISM? No.

It was OK when Wikimedia decided to make a stand on SOPA, b/c SOPA legislation had clear and obvious detrimental consequences on the functioning of Wikimedia.

It is not clear or obvious how PRISM or FISA has negative consequences on Wikimedia. In my view, the Foundation seems to have adopted the role of an internet freedom fighter, wanting to take a stand against anything perceived to threaten web users' privacy and freedoms. Now, that might be an admirable position, but it's also to some extent a political position and one that clashes with the foundation's longstanding principle of remaining neutral on such issues. moved from blog, comment by Nicholas Sammons : 2013/06/14 at 7:59 UTC by Jalexander (talk) 10:11, 15 June 2013 (UTC)

To be neutral about the knowledge inside Wikipedia and being neutral about the way internet works are not the same thing. If we want a neutral point of view inside Wikipedia, we need to protect free use of internet for dissident opinions to be able to exist. I think the Wikimedia Foundation should fight for the freedom of internet. Lionel Allorge (talk) 11:03, 15 June 2013 (UTC)

Staying neutral in the face of a global wiretapping action by the US isn't neutral. Silence means saying "Yes" to this actions. We shouldn't do that. It is pretty clear how Wikimedia is affected by PRISM. It is about trust in internet use at all which then includes the never to be answered question about the tracking of your own search habits on Wikimedia projects.

So I vote Yes for at least joining the public statements and efforts according to the role Wikimedia can do relating to its community's value and mission. --Jensbest (talk) 13:26, 15 June 2013 (UTC)

Then I guess we would all appreciate if you let us know *how exactly* Wikimedia is affected by PRISM and how is it involved in the scandal that broke around it if you think it's *pretty clear*. For me it isn't, so I would welcome an explanation. odder (talk) 13:46, 15 June 2013 (UTC)

You can't look on Wikimedia without reflecting on its digital environment. If the web as a whole is monitored by a state, Wikimedia, with Wikipedia being one of the biggest websites in this web, must take a stand according to its values and long-term practices. It isn't about the question if there is any Wikimedia-Staff forced to lie to us because of secret judge rulings and gag orders, it is about the fundamental question if there can be a free, not-state-monitored encyclopedia in a non-free, state-monitored web. The actions of the US-government spreading massive distrust all over the web. Distrust is endangering the emancipatory and participatory culture of the web which is also an important foundation of all Wikimedia-projects. --Jensbest (talk) 18:28, 15 June 2013 (UTC)

Certainly Wikimedia does not have to do anything. It is the Foundation's (or rather the community's) choice whether to take any action, which is precisely what is being debated here. There is no information whether any

government monitors the whole web, PRISM is only about one government monitoring services of a couple of companies (however big they are). However, it's common knowledge that the Web, or some parts of it, has been monitored and censored for a long time (take China, Qatar, Egypt, Syria, and now Turkey as examples), and the Wikimedia movement did not protest against that. odder (talk) 18:57, 15 June 2013 (UTC)

Certainly Wikimedia has to do something when the country in which most of its servers are hosted is convicted doing massive secret global webwide monitoring. You are wrong on how PRISM works. It is sweeping the web at a whole AND is using direct access to thousands of companies. Therefore my point made above is very relevant - there is no good web use inside a corrupted system, there is no free and anonymous use when the leading country of the so-called free webworld is doing massive global secret surveillance. The other "argument" that the web is partially state-monitored anyway and therefore any action would be useless is definitely the most fatalistic and irresponsible opinion on freedom I've heard for a long time. -Jensbest (talk) 20:52, 15 June 2013 (UTC)

How do you know that? As far as the media report the situation, PRISM is related to a small number of Internet service providers, if you take the global picture into consideration. Plus, I've never said that Wikimedia shouldn't act — I only said that it *did* not act when there were reports on how Chinese, Syrian, Egyptian and now Turkish governments monitored and censored the Web. We have millions of readers in those countries, and yet there wasn't any suggestion for the WMF to join the local initiatives for a free and unmonitored Internet — if we're acting now, then I'd think it be just fair for the WMF to react whenever there are reports on monitoring Internet users in countries reached by our projects. odder (talk) 21:09, 15 June 2013 (UTC)

I agree with you that it is a question of how to balance decisions on taking action. Maybe Wikimedia should have a more fundamental permanent stance on the subject, but being based on the idea of openness and collaboration Wikimedia has to stick to the more complicated and sometimes tedious decision-finding process by asking the community. This doesn't make us as effective and "punchy" as other digital NGOs more focused on fighting for digital rights like EFF etc. - But then again, if this "big ship" Wikimedia is moving it means something for more people even beyond the digital filterbubble. - According to your question about the broadness and depth of Prism and related state-surveillance activities I don't wanna spam you with articles, so just one for some sunday lecture: a longer overview-article by AP . --Jensbest (talk) 22:23, 15 June 2013 (UTC)

One potential argument: Wikimedia relies on editors being able to edit freely without real world retaliation. This is one reason things like no legal threats is a policy. If editors fear retaliation by gov for the things they do on wikimedia, they wont do things that might piss off gov. Amount of systemic bias in Wikimedia could sky rocket. Obviously we arent at full survalience/police state yet, but things like that happen one small step at a time. This is a large step. Bawolff (talk) 15:17, 15 June 2013 (UTC)

- Yes we should decry PRISM, unless that is the US government announces that it wasn't monitoring Wikimedia traffic. If they give an assurance that they weren't snooping on us then Wikimedia should revert to neutrality as that would be consistent with only reacting to direct threats. Decrying is much less drastic an action than a blackout, and I think that it would be an appropriate level of action. WereSpielChequers (talk) 15:01, 15 June 2013 (UTC)
- That's definitely compliant with Wikimedian values and long-term practices: Wiki contributions are based on the premise that we are not forced to disclose our *real* identity. Alexander Doria (talk) 16:07, 15 June 2013 (UTC)
- I applaud the Wikimedia foundation for taking action.

It is to my knowledge that the "collection" of data from those internet companies mentioned in the leaks are not done willingly, but unknowingly through a massive collection of packets that travel to and from their data centers (very similar to the upstream method found here http://en.wikipedia.org/wiki/Room_641A).

If this is true, the only preventative way of circumventing such "prism" taps would entail allocating your data centers, specifically for North America, outside of United States jurisdiction — to Canada and Mexico, for example. However, user packets that are sent to and from Wikipedia are still very vulnerable as they will traverse private ISPs in the U.S., those of which are supposedly already under surveillance.

An immediate response would be implementing a secure SSL connection for users inside the United States.

I hope the Wikimedia foundation, along with other key organizations, continue to fight for a free, open and secure internet.

I thank you all for your efforts. moved from blog, comment by Mark B : 2013/06/15 at 21:47 UTC by Jalexander (talk) 01:07, 16 June 2013 (UTC)

- Yes, the WMF should join with these organizations and support efforts to protect internet privacy from warrant-less removal. - Amgine ^{meta} ^{wikt} ^{wnews} ^{blog} ^{wmf-blog} ^{goog news} 16:35, 16 June 2013 (UTC)
- **⊕ Support** – We should stand with the Internet and against government spying. - -Michaeldsuarez (talk) 23:11, 17 June 2013 (UTC)
- The WMF board should feel free to make a statement, if there is consensus for one, and individual board members should feel free to campaign as individuals as much as they wish, but I would be firmly opposed to a PRISM blackout in the style of the SOPA blackout. While I understand the temptation to wield political power, the project as a whole should not be a political actor, but remain neutral. Andreas ^{UN}466 10:32, 18 June

- 2013 (UTC)
- **Oppose** Per Andreas. --Anthonyhcole (talk) 12:37, 18 June 2013 (UTC)
 - **Oppose** - I believe it's already been acknowledged by the Feds that to the extent that info is being collected beyond that pursuant to a particularized request, it's because they are data mining and data mining more or less by definition means the queries are not particularized. I don't think people fully understand just how different this is from prying eyes reading your personal email. On the other hand, were the WMF to gain media attention for its activism here, in my view it would provide some evidence for my claims at the the time of the SOPA/PIPA activism that the WMF feels compelled to weigh in on civil liberties issues that are of dubious if any connection to the development of Wikimania projects.--Brian Dell (talk) 18:44, 19 June 2013 (UTC)
 - **Comment**. WMF needs to find out, in detail, whether any of these programs **potentially** affect Wikipedia, which is a different question from whether information has been delivered so far. My assumption is that potentially yes, they could be served up a NSL tomorrow demanding data on everybody who reads w:Acetone peroxide, etc. Indeed, it seems too tempting a resource for me to be entirely credulous that the NSA has passed it up so far - surely there were a few days a while back when they would have wanted every possible means to know who looked up anything about pressure cooker bombs from an IP address in Boston. In opposing this, we oppose what seems like a very sensible police tactic, and we have to do so on the basis of weighing the mild harm against the vast multitude against the chance of preventing grievous harm to a few - and in an age of locking down a whole city, there are clearly some authorities making the wrong decisions about things like that. We'll need more transparency about how search warrants/subpoenas for such things are *legally* delivered, and what protections there are there. What we need here isn't a vague feeling, but a well-constructed ideological fortress. We just need a lot better data and thought about all the issues involved. It is unfortunately likely that, far from being on the offensive, Wikipedia will find itself trying to argue against *mandated* data retention policies that have been promulgated in many contexts, trying to preserve what it has now. Wnt (talk) 21:48, 19 June 2013 (UTC)
 - **Support** Prism (according to some people) presumptively examines all Wikipedia traffic (along with all other internet traffic) from Room 641A and similar locations. Therefore its operators monitor everything everyone is reading (even if only metadata is logged, that is enough to deduce the content being read, from message sizes). This has potentially major consequences for readers and therefore is a matter of serious concern for Wikipedia. Even if the allegations turn out to be false, they are plausible enough to have a chilling effect in their own right, so Wikipedia should intervene either way. I personally support major changes in Wikipedia operations and practices to deal with this, but that's beyond the scope of this immediate question. 50.0.136.106 07:14, 20 June 2013 (UTC)
 - **Support**. I don't fear US where I'm located in France. Though I still fear blanket cooperation of France with US to provide everything that US requests. But I would need to violate French laws. I don't fear the consequences of my opinion and I'm free for reading everything I want. But I stil think that users around us are in severe troubles, and US action will create a precedent that will be followed by other countries (notably in

China, and in all Islamic countries, as well as Russia, against their political opponents; LGBT people for example are in severe troubles now almost everywhere in Africa, Russia, Central and Southern Asia, Indonesia, only by the fact they may read about these topics or give their opinion, or present the facts about what happens in their country, or translate articles about their country originating from foreign countries into their national language : this is even more critical for languages that are not major, like Azeri, Uzbek, Burmese, Persian, Urdu, Indonesian/Malaysian, Javanese... and most African languages, because there's not a very active and protected community abroad using these languages on Wikimedia projects... If people in these countries cannot read major foreign languages, they will be presented a skewed view. This view will be skewed (NPOV) even in Wikimedia sites edited mostly by other national residents of their country). verdy_p (talk) 00:26, 21 June 2013 (UTC)

Update [edit]

Hello all, thank you to everyone who shared their feedback above. Based on this consultation, there is limited support for advocacy about government surveillance, such as PRISM. We are currently evaluating possible advocacy options that are consistent with this feedback. Particularly, we are looking for options that are focused on government surveillance from an international perspective. You are welcome to continue to leave feedback and suggestions, and I will keep you updated. Thanks again, Stephen LaPorte (WMF) (talk) 18:52, 5 July 2013 (UTC)

15 threads, 10 support, 1 comment, 4 oppose (66.7%, 6.7%, 26.7%) - Amgine/meta wikt wnews blog [wmf-blog](#) [goog news](#) 17:28, 8 July 2013 (UTC)

But also a fair amount of negative feedback in other parts of the discussion (e.g., "US Issue" below, some of the blog comments), so my sense is that a pure count of the (very small) numbers does not mean much. Honestly open to persuasion/discussion on that point, though. LVilla (WMF) (talk) 17:39, 8 July 2013 (UTC)

Actually, I took the liberty of examining the remainder of this page. Not one thread did I find which stated opposition to action on this topic. There were questions about whether this is a solely US topic (which, in a manner of speaking, it is, as it's the US NSA whose actions are being discussed.) There were discussions which suggested this is diversionary. But none opposed acting on it. Perhaps you're referring to discussions elsewhere and ascribing them locally as none expressed opposition to acting on this topic as far as I could discern. -

Amgine/meta wikt wnews blog [wmf-blog](#) [goog news](#) 07:03, 9 July 2013 (UTC)

If we feel that "stopwatching.us" is too US-centric, I think it would be appropriate for us to post a similar statement of our own, framed more globally:

- Indicating that we will support regional or national efforts to keep this aspect of the web open, because of its impact on the free exchange of knowledge.
- Listing the national/regional initiatives we are aware of, which we may or may not have expressly signed on to.
- Listing and amplifying the participation of Chapters and other regional Wikimedia groups who have supported those regional initiatives.

• Encouraging the global Wikimedia community to help keep the Web open in this fashion.

–SJ talk 18:34, 8 July 2013 (UTC)

Stop logging IP addresses [edit]

Currently and as far as I'm aware for the life of the project, edits by IPs have been publicly and permanently logged by full IP address on our databases. For me as a Brit that has never been an issue, and I even linked a couple of IP addresses I'd used in one of my RFAs. But to others it is an ongoing issue, I gather that much of our oversighting relates to accidentally disclosed IPs. IPs present a real security risk, for example an IP editor in a totalitarian country might not be aware of what irritates the regime, might be unaware that their IP is so easily tracked to them, might be caught out by an unexpected change of regime or may simply lose their temper and say something that puts them in trouble. We could fairly easily reduce these risks this by assigning temporary codes to IPs that edit. Unless there were a block in place, the codes could be reset every few months. Checkusers would still be able to look at recent full IP addresses. Other editors could still see which other edits had been made by the same IP during a period of months. But once the codes changed even the checkusers would only be able to link the IP addresses of last few months edits to defunct temporary codes, much as is the situation with logged in editors. Arguably the US would be the Government least affected by this security measure. But a boost to the security of an oft neglected part of our community would be a reassuring response to PRISM.

WereSpielChequers (talk) 15:41, 15 June 2013 (UTC)

Stopping logging IP's will be a problem for the fight against spammers. But a solution is would be to transfer all logs outside US in a safe haven, in compressed batches, leaving just the minimum logs needed for performance, on a short timeframe.

However the US law may still already require that service providers keep a minium amount of logs for inspection. In all cases, these logs must be severely restricted from random accesses, kept on servers in encrypted forms. And most probably, there should no longer be any user with CheckUser capability ni US or acting under US law.

Note that many other countries already have such laws requiring keeping a minimum amount of logs for judiciary requests. In some countries this could be just a couple of months, in some others the requirements may extend to several years. For very visited sites, this means a cost not only for the storage, but also to ensure that it will be correctly backed up and saved from severe crashes, so that they remain readable (this implies additional maintenance costs for these backups, possibly offsite, or could require transferring these logs to a legally approved legal escrow, that will also want to be paid for this service... or directly to a governmental department).

For now the WMF is locating most of its servers in Florida and has to comply to the laws of US and Florida (some servers for tools or for proxies are also located in Europe : proxies also may need to keep these connection logs.

In some countries, users already can only to Wikimedia sites by using mandatory national proxies). Most users accessing to WMF sites via mobile Internet accesses are also using proxies maintained by their ISP, which will keep these logs (in addition to restricting the protocols, for example only HTTP, or HTTPS only for authentication and

data signatures for securing commercial bank transactions, but not strong encryption!). But the scope of PRISM is not just about connection logs to help tracking network paths and identify the senders. It is really in inspecting the contents sent, and getting access to the full user profiles maintained by websites (for example the full list of emails sent and received with their content and metadata, and precise timing of user interactions with any online service : this includes the Internet, as well as GSM networks or any other electronic transport path).

The solution would be transmit data hidden within analog signals or strong random noise fields with steganographic technics (those that are used by militaries that can hide their transmission within the mediums used by regular commercial channels, by slightly modifying it in an invisible way (a way that does not break the existing protocols, or that just generates a small amount of random errors that these networks tolerate.) But Wikimedia is not a military organization, and these technics are very costly (they constantly need to be adapted, this implies huge unamortized development costs).

verdy_p (talk) 16:29, 15 June 2013 (UTC)

Note, one has to be careful when designing such a system, as it is shockingly easy to design something like that poorly, and have it be no more private then just putting the IPs of anons everywhere. Historically, if you go back far enough (aka during phase 1 time), we actually blanked out the last 3 digits of the IP address so it was just xxx. (AFAIK we stopped because this didn't actually provide any "real" privacy). A second problem is that each IP address is not an independent number, they are related. If we replaced each IP with some sort of hash of the IP, we wouldn't be able to as effectively investigate vandalism that comes from different IPs from the same network. Range blocks also would be a thing of the past. Bawolff (talk) 18:16, 15 June 2013 (UTC)

Good points, yes a careful redesign would be needed, and we still need to retain the ability to rangeblock. I think it is time for a major review of this area, both for privacy and to reduce collateral damage. For example range blocks are notorious for effecting lots of innocent parties, *smart rangeblocks* would only block edits by people with the same hardware and and browser configuration as the problematic editor. WereSpielChequers (talk) 23:55, 15 June 2013 (UTC)

I'm inclined to agree with WSC about this, but honestly -- I always assumed the reason why Wikipedia lists the IP addresses openly was to spare government agents the trouble of coming in and requesting them (and themselves the trouble of giving them out). Wikipedia's structure has in many ways seemed like a reaction to long-term spying, where so little is kept that is *not* public that the spies barely have an advantage over anybody else, which may be the best anyone can achieve now. Wnt (talk) 21:51, 19 June 2013 (UTC)

We have no longterm need for most IP data, and the spies can't request what no longer exists. OK there are some scenarios where this would be of little use, but what about where governments change and a new government wants to know things that one could have trusted the old government not to ask? WereSpielChequers (talk) 12:13, 30 June 2013

"law-enforcement agency or a court or equivalent government body" [edit]

http://wikimediafoundation.org/wiki/Privacy_policy uses "law-enforcement agency or a court or equivalent government body" language. Does that include the en:National Security Agency ? Teofilo (talk) 18:56, 15 June 2013 (UTC)

A U.S. issue? [edit]

The fact that WMF is concerned about privacy-eroding actions by the U.S. government is commendable, and I completely agree with ALA's statement quoted in the blog post: "rights of privacy are necessary for intellectual freedom". I also agree with the statement that "the global nature of internet traffic, and the alleged sharing of surveillance information between governments, means that Internet users around the world are potentially affected". However, as far as the issue has been handled by the organisations in the *StopWatchingUs* coalition up to now, the matter falsely seems to be only affecting U.S. citizens. We, non-U.S. citizens, have been ever treated as second-class humans in U.S. law: the safeguards against illegal wiretapping in FISA and PATRIOT act only apply to U.S. citizens. And despite the fact that the alleged surveillance potentially affects hundreds of millions of people around the world, the *StopWatchingUs* coalition is calling to "*Enact reform this Congress to Section 215 of the USA PATRIOT Act, the state secrets privilege, and the FISA Amendments Act to make clear that blanket surveillance of the Internet activity and phone records of any person residing in the U.S. is prohibited by law and that violations can be reviewed in adversarial proceedings before a public court*". That would surely be a good step forward for U.S. citizens, but still leaves out in the cold us. By "us", I mean the people *from abroad the U.S.* that access the Internet *from abroad the U.S.* to send contents to or retrieve them from *abroad the U.S.* and whose packets are routed through the U.S. (as 60 % of Internet traffic does). If WMF intends to push a less U.S.-centric approach in this issue, please count with all my support. But, please (and perhaps once in a lifetime), please stop seeing U.S. as the very center of the Universe. Thanks, Cinabrium (talk) 23:10, 15 June 2013 (UTC)

Blanket surveillance of the use of US servers is a global issue. The language of this page does not suggest otherwise. We should focus on the underlying principles of privacy, which are universal. –SJ talk 23:48, 15 June 2013 (UTC)

@Sj But the letter by StopWatchingUs does *not* focus on "underlying principles" but on some aspects of US law only affecting US citizens. That was Cinabrium's point. –Chricho (talk) 01:15, 16 June 2013 (UTC)

Exactly. Thanks, Chricho. Wikimedia projects house a huge international community, which is affected by U.S. surveillance policies (and in a non trivial number of cases, by those of their home countries too). If WMF's actions on this issue will be limited to endorse the *StopWatchingUs* letter, then nothing would have changed for those member of the community out of the U.S. Furthermore, while demanding transparency and respect for privacy from the U.S. government,

and taking into consideration the transnational nature of the community, WMF should engage in similar actions wherever privacy and freedom of expression are harmed by sevetive laws and Star Chamber procedures. Canada, Sweden, Italy and India are just examples of legal frameworks allowing forms of surveillance even more invasive that those in the U.S. I'm not opposing actions with regard to NSA's PRISM scandal (I would add BLARNEY, NUCLEON, and many other questionable systems). I'm just saying that WMF's actions should be directed to protect some fundamental rights of the whole Wikimedia community, wherever those rights may be at risk. Cinabrium (talk) 08:56, 16 June 2013 (UTC)

Hello, Alex Fowler here from Mozilla, one of the sponsoring organizations behind the StopWatching.Us campaign. We are also a community made up of thousands of contributors from around the world. Starting this week, we've broadened the campaign site to be inclusive of citizens outside of the US. More is underway to broaden input and dialogue from around the world. We'd benefit greatly from this community's participation and ideas on other ways to globalize campaign messages and actions.

Hello, Alex! Endorsing this statement (and convincing other organizations to do the same) could be a good starting point for globalizing the campaign. Cinabrium (talk) 17:38, 19 June 2013 (UTC)

I agree with Cinabrium's and Chricho's remarks. --NaBUru38 (talk) 20:34, 18 June 2013 (UTC)

Comments copied from Blog [edit]

- The united states government is only trolling the very low hanging fruit. Any serious netherios group knows the ways to circumvent detection. Its reminiscent of "weapons of mass destruction" and will be lapped up by the chattering classes on the net.

Anonymous. Copied from blog; Comment by Anonymous 2013/06/15 at 00:37 UTC by Jalexander (talk) 07:57, 16 June 2013 (UTC)

- What people want to know is this:

"When I read Wikipedia is the government reading over my shoulder, logging my activity, and potentially inferring my politics and values?"

But they cannot find the answer to this simple question in your post. Allow me to help you with a frank answer:

For some users the answer is unequivocally yes: Wikimedia has *_specific_* knowledge of authorities in some countries intercepting and monitoring traffic to Wikipedia.

For users who are concerned about observation by the US government the frank answer is "We probably couldn't tell you if it were so, so asking us is pointless."— if Wikimedia was ordered to lie by the United States government it would lie. It might fight such an order but it would lie until it won. Furthermore, individual members Wikimedia staff may also be acting under the influence of the US or other government without Wikimedia's knowledge. It is difficult to be sure of the absence of surveillance.

Wikimedia also currently keeps detailed access logs which may be subpoenaed (or stolen)

at some time in the future and used to look for people (by IP address) were reading particular articles or which articles a particular IP address has read. Similar data— in the form of search engine logs— has been used in US courts in the past to prosecute people.

Fortunately the readers of Wikipedia aren't helpless and don't have to trade privacy for knowledge:

- If you use the [https-everywhere](https://www.eff.org/https-everywhere) browser add-on (<https://www.eff.org/https-everywhere>) the identify of the specific articles you read are hidden from any party who does not have Wikimedia's cooperation.
- If you browse using Tor (<https://www.torproject.org/>) then your Wikipedia reading habits will be kept more private even if Wikimedia is cooperating with parties conducting surveillance, and the fact that you are using Wikipedia at all will be hidden.
- For smaller Wikipedia languages it is feasible to download the entire Wikipedia and read it offline at your leisure (http://en.wikipedia.org/wiki/Wikipedia:Database_download)

You can also limit your Wikipedia browsing to public wifi networks, although many keep logs, and libraries systems where no identification is required.

These actions can keep your reading private regardless of the specific surveillance program of concern or Wikimedia's level of (non)-participation. Copied from blog; Comment by Greg Maxwell 2013/06/15 at 01:21 UTC by Jalexander (talk) 07:57, 16 June 2013 (UTC)

- The US government doesn't believe in humans, their values. So the PRISM happened. Copied from blog; Comment by arun 2013/06/15 at 03:59 UTC by Jalexander (talk) 07:57, 16 June 2013 (UTC)
- About note 2: it has been revealed that the alleged minor limits on the scope of surveillance only applies to US nationals living in US, but in fact this is only determined by a fuzzy reasonable conviction that the location and nationality Internet user is not really very well determined. These fuzzy limits imply that more than half of US citizens will be spiable independantly of these limits.

The limitations of budgets for the US agency means that they will in fact just scope some keywords to determine this.

In addition this minor limitation of sope also means that US citizens located abroad, or accessing the Internet via foreign networks will be spied without knowing it. As well, the world traffic from abroad that can reach a US network is tremendous, due to the many third-parties involved in delivering Internet services in the world. So anyone in the world will not be subject to these limitation of scope, and can have their personal data or opinion gathered, stored, and searched in the US agency "Big Data" systems, and kept for unlimited time.

There's absoutely no limits on the usage that will be done about these data, and it may be used to exercise pressures against people around the world, only for their political, social or economical views or actions, even if these actions are perfectly legal in these countries (and rules there by laws protecting their privacy). This could then be used not

just for fighting against terrorism or international criminality (this is already allowed within international cooperations of law enforcement polices, under the scrutiny of national justice systems), but for any concern that the US government judges will be useful to protect its own economical interests, such as limiting the capability of selling things to US, or threatening them of nex taxes, or harassing their contacts in US that still work there in full compliance with US laws (for example refusing to contract with them, without having to justify why).

We've already seen people denied access to US when boarding a plane or only when they put their first foot on a US airport, for many false (unverified) allegations of links with terrorists, or international criminals, or their providers, only because they had a name similar to a growing list of people created in a multi-level web where those people have never had any contact or nay reason to believe that they were in contact with these seeked people. Every month now, this costs a lot of money to travel agencies around the world (or in US), and people are held in custody temporarily and ejected back to their country, based on false allegations or suspicions. And legal contracts are broken unilaterally by the US government? All these actions are made without any compensation (people may only defend their case in a US court, but they cannot go there and the only mean for them would be to pay a very costly US attorney, acting alone with very limited informations collected : only rich people can pay these services, without any warranty that false allegations or suspicions will be removed from the databases, and new difficulties will reappear later, even if the initial allegations were proven completely wrong).

On the opposite, the US in fact does not collaborate with the same scale to fight against some US criminals, and offers a passive protection in many cases, not really limiting their actions (notably in cases of financial abuses and Internet abuses).

It is wellknown that US even pays them to act abroad, and will protect them by offering them immediate asylum in US in case of problems, and that legal threats against them abroad will be alerted to them, to limit the legal actions or embarass the investigators (using private information collected illegally from them, without them having any action in US, or against US, or being aware that this may impact some US politics or interests, other than fair and legal competition protected by international treaties and conventions).

This system of Internet surveillance is very unbalanced when we measure how the Internet is controlled from US, or its services are hosted in US for most critical operations, as well as a broad cloud of third-part providers of services (and of proprietary softwares, hardwares and very important technologies such as encryption, DRM systems, the PKI... and even HTTPS itself). The US detains the power-off button to cut any one at any moment from most parts of the Internet (even on services made abroad and not intended really to be used in US). The core infrastructure of the Internet cannot work without US control (or it can only work in a very limited subnetwork, but not on the "open" Internet we use everyday via our foreign ISPs, that are often liable themselves in US where they have some subsidiaries, and via international stock markets controlling their corporate governance).

For these reasons, your note #2 tends to reduce the severity of the effective impact of

this surveillance. Probably only about 100 millions of US citizens will be protected, within a world of 7 billions people (this is about 98.5% of the world population that will be under possible US scrutiny of their legal private life, at any time and for no reason at all at the time of this surveillance, but who will become some years later to difficulties or personal harassment...) Moved from blog comment by Verdy_p on 2013/06/15 at 09:45 (UTC) by Jalexander (talk) 01:20, 16 June 2013 (UTC)

PRISM concerns Trust, Trust concerns Wikipedia [edit]

I strongly support any steps by the Wikimedia movement (including WMF) to openly oppose PRISM and similar spy programs. Though currently there is little certainty about what exactly is happening, it is clear to me that NSA spying has the *potential* to violate privacy rights of our users on a massive scale. As a main source for unbiased and quality information on the web, there is every reason to believe that Wikipedia is a potential target. Among the billions and billions of harmless requests, there are without doubt some interesting ones, to filter out which is the NSA's specialty. Someone from the middle east is acquiring chemistry knowledge on Wikipedia that could be helpful in making bombs? A French author writes elaborate articles about military radio stations? The simple fact that most of what is accessed is harmless does not mean that everything is.

As a result, the privacy of our users is in jeopardy. Even if you don't agree with this, certainly the *belief in privacy* is in jeopardy. If users can't or won't trust us anymore to distribute uncensored information in a privacy-respecting manner, this is a huge loss. It is our responsibility to make sure that users can and will keep trusting and that their trust is well-founded by doing everything in our power to make sure our user's rights are respected. - Tobias talk · contrib 23:00, 16 June 2013 (UTC) Ps.: The big Internet companies are busy finding sneaky wordings that dodge the question of whether violated user privacy. With SOPA and PIPA there was a broad alliance. With PRISM, much more depends on our voice.

Saying Wikimedia ought to take a stand whenever "the *belief in privacy* is in jeopardy" would seem to place an extraordinary burden on the foundation. One could point to a whole slew of legislation/government practices which potentially threaten the *belief in privacy*. Is Wikimedia's role that of some kind of privacy warrior akin the ACLU? NickCT (talk) 14:46, 17 June 2013 (UTC)

Sorry, I should have been more precise. I'm talking about privacy *when accessing Wikipedia*. Facebook and Google doesn't respect user privacy, that much is well known and it shouldn't be a great concern to Wikipedia/Wikimedia. Similarly, if the government decides to install more CCTVs, it doesn't impact Wikipedia directly. But with PRISM and other governmental spying activities, privacy not only of our users in general, but *while browsing Wikipedia* is at stake. --Tobias talk · contrib 18:48, 17 June 2013 (UTC)

Snowden as Wikimania keynote speaker [edit]

In August we will have Wikimania in Hong Kong and I would like to hear Snowden. (If it is secure for

him.) This would be also a good statement, beside joining stopwatching. So please invite him. -

-Kolossos (talk) 18:39, 17 June 2013 (UTC)

+1 --Kellerkind (talk) 19:00, 17 June 2013 (UTC)

+1 --Tobias talk · contrib 19:46, 17 June 2013 (UTC)

+1 --Manastirile (talk) 20:14, 17 June 2013 (UTC)

+1 -- TheOriginalSoni (talk) 04:20, 18 June 2013 (UTC)

+1 but not billed as a "keynote speaker". That's too big a statement, and I'd be very uncomfortable pinning our public face to this issue. While it's relevant, important, appropriate and will surely catch the media, our core Wikimedia priorities include our own affairs - Wikipedia Zero, global south, editor rates, Wikimedia community, Visual editor, and chapter and foundation highlights of the year. If we include a prominent but not keynote session with him, that doesn't dominate our core issues, that would come across better and more maturely - and not like bandwagon jumping. It won't go un-noticed for low-keying it. FT2 (*Talk | email*) 13:32, 18 June 2013 (UTC)

I don't imagine this will be possible. It seems as though Mr. Snowden is currently in hiding. I imagine by August he'll be in a U.S. prison or dead. --MZMcBride (talk) 16:50, 18 June 2013 (UTC)

...or in Iceland at the Blue Lagoon <:o) --Kellerkind (talk) 18:34, 18 June 2013 (UTC)

If it's unsafe for him to come personally, can he give a speech through Skype or something Ypnypn (talk) 22:26, 18 June 2013 (UTC)

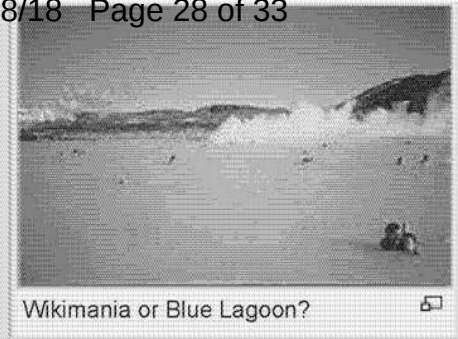
+1, A dedicated speech will be more than enough. Chenxiaoqino (talk) 13:00, 19 June 2013 (UTC)

+1. I would suggest that he should be strongly encouraged to spend at least *some* time talking about how NSA surveillance affects Wikimedia projects in particular. In this way, such a talk can be viewed not solely as a political statement but as a technical consultation, and if an honorarium is required it would be more feasible to justify the spending on that basis. Wnt (talk) 21:23, 19 June 2013 (UTC)

- Though I should emphasize about the above that some good lawyers had better check over everything carefully - we would not want Wikimedia to end up with Assange-like charges of actually paying for/conspiring in *new* releases of classified information. Wnt (talk) 21:33, 19 June 2013 (UTC)

Historical Background [edit]

See also w:Cabinet noir. One of the best things Wikipedians can do about this issue is to provide professional, serious, published knowledge about this issue in its articles. Teofilo (talk) 22:00, 17 June 2013 (UTC)



Wikimania or Blue Lagoon?

[edit]

Call for input on WMF privacy policy

Not the same topic but related in many ways so I wanted to drop a note here pointing to the new Call for input on WMF privacy policy (also posted as a blog post) and it's associated discussion page. Jalexander (talk) 09:41, 19 June 2013 (UTC)

Universal Declaration of Human Rights [edit]

« No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks. » (article 12).

Does anybody remember the Declaration of the Independence of Cyberspace? It was in 1996. Twenty years later, non-free software providers let governments to read everybody's emails, phone calls, web access... This is not only an attack against human rights, but also a threat to the knowledge society. Privacy is a pillar of liberty, a need on Internet. And without freedom, no free software. Mediawiki is free software, and our free encyclopedia is online.

We have to support our allies. (GENIUM) 21:48, 20 June 2013 (UTC)

and now? [edit]

A decision should be reached on the 21th June, now is the 25... Any news on the subject? -Isderion (talk) 01:38, 25 June 2013 (UTC)

Hello Isderion, we are reviewing the above comments, and we will share an update soon. Many thanks, Stephen LaPorte (WMF) (talk) 16:23, 25 June 2013 (UTC)

Soon? --Kellerkind (talk) 14:12, 2 July 2013 (UTC) P.S. If you don't like to do something, that's ok, but say something.

This is getting frustrating. You give the community one week to comment, the community participates to a small degree and then you need more than 2 weeks for reviewing the comments and reaching a decision. In the meantime you give no information to the community. This is not my understanding of a professional community liaison. --Isderion (talk) 23:14, 4 July 2013 (UTC)

Is there anything I can do to help here? I also haven't heard any update but, as I noted more generally here, I feel it is important to our community and to our long-term mission for us to take a stand beside like-minded organizations. I would like to help the WMF take a more public stance on the matter. -SJ talk 20:55, 7 July 2013 (UTC)

Thanks for the offer (and btw. congrats for the board seat), but the WMF posted an update 2 days ago, though it is a little bit hidden in the middle of the page (see Talk:PRISM#Update). It seems that this topic is rather low priority for the WMF, but I appreciate that they are going to focus on an international perspective, now that it becomes more and more clear that most governments spy on each others citizens and sometimes also their own. Maybe Noam Chomsky is right when he says that Governments will use whatever technology is available to combat their primary enemy – their

PRISM in not everthing [edit]

Now we have also a problem with British GCHQ so the problem comes to europe. And there are also articles about surveillance of public social media

<http://www.wired.co.uk/news/archive/2013-06/26/socmint> and other stuff. So should we have different pages, should we have a more generally page or should we still concentrate on US-GOV and PRISM? --Kolossos (talk) 22:02, 26 June 2013 (UTC)

Government surveillance? --Kellerkind (talk) 11:52, 27 June 2013 (UTC)

Wikimedia may be lying [edit]

It is of knowledge of everyone that US authorities have, nowadays, power enough to make secret subpoenas, that means, request user's informations without user's knowledge, and without and order from a judge. The holder of the information may be arrested and suffer bitter consequences from revealing information about the subpoena to the targeted user. That said, subpoenas may have been sent to Wikimedia Foundation, and if it is forbidden to reveal any cooperation with US authorities, it's completely useless to simply state that it did NOT cooperate with them. Useless, and senseless, for the simple fact that it would be a crime to admit the oposite. That said, it is clear for me that it is **NOT** safe to trust in ANY organization, foundation or enterprise located in the US, or owned by any US organization, foundation or enterprise. US has become a state of exception, and the most realistically measure to be taken would be moving not only servers, but also capital, staff and headquarters to places where freedom of expression still has some meaning.

- AFAIK with open source software it's harder to hide secret measures to record information than with closed source software. The Wikimedia software on this site is open source. It's why hackers didn't trust Michael Domscheit-Berg when he refused to release the source code for his "en:OpenLeaks" website. WhisperToMe (talk) 15:02, 6 July 2013 (UTC)
 - It is possible for certain requests (*national security letters*, which are different than a subpoena) to include a demand that you not tell anyone you have received one. However it does not compel you to lie; you can simply say you "cannot answer" when asked whether you have received one. In contrast, until an organization has received such a request, it can say clearly that it **has not** received such a request. Wikimedia's head counsel stated clearly on the blog, "*We have not received any National Security Letters*." (Caveat: as a Board member, I would not be notified if such an NSL had been received by the Foundation, so I have no direct knowledge.) –SJ talk 20:55, 7 July 2013 (UTC)

The above discussion is preserved as an archive. Please do not modify it. Subsequent comments should be made in a new section.

Further feedback and suggestions [edit]

Hello all, thank you to everyone who shared their feedback above. Based on this consultation, there is limited support for advocacy about government surveillance, such as PRISM. We are currently evaluating possible advocacy options that are consistent with this feedback. Particularly, we are looking for options that are focused on government surveillance from an international perspective. You are welcome to continue to leave feedback and suggestions, and I will keep you updated. Thanks again, Stephen LaPorte (WMF) (talk) 18:52, 5 July 2013 (UTC)

15 threads, 10 support, 1 comment, 4 oppose (66.7%, 6.7%, 26.7%) - Amgine/^{meta wikt}
 wnews blog ^{wmf-blog} ^{goog news} 17:28, 8 July 2013 (UTC)

But also a fair amount of negative feedback in other parts of the discussion (e.g., "US Issue" below, some of the blog comments), so my sense is that a pure count of the (very small) numbers does not mean much. Honestly open to persuasion/discussion on that point, though. LVilla (WMF) (talk) 17:39, 8 July 2013 (UTC)

Actually, I took the liberty of examining the remainder of this page. Not one thread did I find which stated opposition to action on this topic. There were questions about whether this is a solely US topic (which, in a manner of speaking, it is, as it's the US NSA whose actions are being discussed.) There were discussions which suggested this is diversionary. But none opposed acting on it. Perhaps you're referring to discussions elsewhere and ascribing them locally as none expressed opposition to acting on this topic as far as I could discern. - Amgine/^{meta wikt} wnews blog ^{wmf-blog} ^{goog news} 07:03, 9 July 2013 (UTC)

As one of the first commenters on this page, I said:

"This certainly seems like a fad issue. [...] I think working on documents such as User:Sue Gardner/Wikimedia Foundation Guiding Principles is a much better use of time and other resources. This allows us to define what we stand for and what we believe, rather than simply denouncing whatever the latest government abuse (or potential future abuse) happens to be in the news at the moment (SOPA, PRISM, etc.)."

If this isn't explicit enough to rise to the level of stated opposition to action on this topic, let me know and I can rephrase.

Another comment copied over to this page reads:

"Should Wikimedia join in decrying PRISM? No."

Given comments like these, I'm not sure what opposition to action would look like to you.

It would be helpful if you could describe specifically what actions you feel the Wikimedia Foundation should take and how you feel those actions would further the Wikimedia Foundation's mission. I think most Wikimedians strongly disagree with secret government surveillance programs such as PRISM. But what of it? Wikimedia is in the business of providing free educational content to the world, not acting as a freedom fighter or political advocate. --MZMcBride (talk) 19:43, 10 July 2013 (UTC)

If we feel that "stopwatching.us" is too US-centric, I think it would be appropriate for us to post a

- Indicating that we will support regional or national efforts to keep this aspect of the web open, because of its impact on the free exchange of knowledge.
- Listing the national/regional initiatives we are aware of, which we may or may not have expressly signed on to.
- Listing and amplifying the participation of Chapters and other regional Wikimedia groups who have supported those regional initiatives.
- Encouraging the global Wikimedia community to help keep the Web open in this fashion.

–SJ talk 18:34, 8 July 2013 (UTC)

I think making a public statement that is less US-centric is fine as well and more in line with our global mission. --Tobias talk · contrib 11:31, 13 July 2013 (UTC)

Followup blog post [edit]

FYI, the Foundation/LCA wrote and posted a followup post on this topic^[?] on July 18.

We should sign the global Principles on Surveillance guidelines [edit]

A coalition of global groups, called "Necessary and Proportionate", formulated a beautiful and non-nation-specific set of guidelines for how to apply human rights principles to surveillance.

It is called the "**International Principles on the Application of Human Rights to Communications Surveillance**^[?]", and has been signed by hundreds of organizations^[?], including human rights, internet, legal, policy, and knowledge organizations. This would be an excellent and appropriate statement for us to sign.

We would be the largest website to sign on to date; but dozens of major global organizations and foundations that we rely on and work with have already done so. –SJ talk 00:56, 7 November 2013 (UTC)

I am very supportive of this suggestion. How can we learn what is the status of the Foundation's decision-making on this suggestion? - Amgine/^[?]meta wikt wnews blog^[?] wmf-blog^[?] goog news^[?] 04:57, 6 December 2013 (UTC)

Meu temor(como brasileiro): [edit | Add topic]

- Eu acho que o governo americano podem invadir conta de administradores da wiki e destruir este projeto. Por isso defendo que sites como o nosso tenham o sistema de segurança EV-SSL. João bonomo (talk) 17:13, 19 July 2013 (UTC)
- I think the U.S. government can invade the wiki administrators account and destroy this project. therefore argue that sites like ours have the security system EV-SSL. João bonomo (talk) 17:13, 19 July 2013 (UTC)

This page was last edited on 6 December 2013, at 04:57.

Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. See Terms of

[Privacy policy](#) [About Meta](#) [Disclaimers](#) [Developers](#) [Cookie statement](#) [Mobile view](#)



Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 14

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
<i>ODNI Interrogatory 19(a)</i>	<i>ODNI Interrogatory 19(b)</i>		<i>ODNI Interrogatory 19(c)</i>	<i>ODNI Interrogatory 19(e)</i>	<i>ODNI Interrogatory 19(d)</i>	<i>ODNI Interrogatory 19(d)</i>
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						
<i>Total HTTP & HTTPS requests: foreign users to WMF US servers</i>	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	
<i>Total HTTP & HTTPS requests: US users to WMF foreign servers</i>	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	
<i>SMTP communications: foreign users to WMF US servers</i>	Unknown		Unknown	208.80.152.0/22, 2620:0:860::/48, 2620:0:861::/48	Unknown	
Category 2 Wikimedia's internal log communications						
<i>Apache Kafka log communications transmitted from WMF foreign servers to WMF US servers</i>	736,045,377,450	Aug. 1, 2017, to Jan. 31, 2018 (six months)	Netherlands	10.0.0.0/8, 2620:0:860::/48	736,045,377,450 log communications encrypted using IPSec	
Category 3 Communications by Wikimedia staff						
<i>Logged international TCP connections using WMF Office Network or WMF VPN</i>	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.

<i>Logged international UDP connections using WMF Office Network or WMF VPN</i>	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.
<i>Logged international ICMP connections using WMF Office Network or WMF VPN</i>	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.

EXHIBIT A

~~HIGHLY PROTECTED - ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

List of Countries with HTTPS Requests to Wikimedia Servers in United States from August 1, 2017 to January 31, 2018

1.	Afghanistan
2.	Åland
3.	Albania
4.	Algeria
5.	Andorra
6.	Angola
7.	Anguilla
8.	Antigua and Barbuda
9.	Argentina
10.	Armenia
11.	Aruba
12.	Australia
13.	Austria
14.	Azerbaijan
15.	Bahamas
16.	Bahrain
17.	Bangladesh
18.	Barbados
19.	Belarus
20.	Belgium
21.	Belize
22.	Benin
23.	Bermuda
24.	Bhutan
25.	Bolivia
26.	Bonaire, Sint Eustatius, and Saba
27.	Bosnia and Herzegovina
28.	Botswana
29.	Brazil
30.	British Indian Ocean Territory
31.	British Virgin Islands
32.	Brunei
33.	Bulgaria
34.	Burkina Faso
35.	Burundi
36.	Cabo Verde
37.	Cambodia
38.	Cameroon
39.	Canada
40.	Cayman Islands

~~HIGHLY PROTECTED - ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

41.	Central African Republic
42.	Chad
43.	Chile
44.	China
45.	Christmas Island
46.	Cocos [Keeling] Islands
47.	Colombia
48.	Comoros
49.	Congo
50.	Cook Islands
51.	Costa Rica
52.	Croatia
53.	Cuba
54.	Curaçao
55.	Cyprus
56.	Czechia
57.	Denmark
58.	Djibouti
59.	Dominica
60.	Dominican Republic
61.	East Timor
62.	Ecuador
63.	Egypt
64.	El Salvador
65.	Equatorial Guinea
66.	Eritrea
67.	Estonia
68.	Ethiopia
69.	Falkland Islands
70.	Faroe Islands
71.	Federated States of Micronesia
72.	Fiji
73.	Finland
74.	France
75.	French Guiana
76.	French Polynesia
77.	French Southern Territories
78.	Gabon
79.	Gambia
80.	Georgia
81.	Germany
82.	Ghana
83.	Gibraltar

~~HIGHLY PROTECTED - ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

84.	Greece
85.	Greenland
86.	Grenada
87.	Guadeloupe
88.	Guatemala
89.	Guernsey
90.	Guinea
91.	Guinea-Bissau
92.	Guyana
93.	Haiti
94.	Hashemite Kingdom of Jordan
95.	Honduras
96.	Hong Kong
97.	Hungary
98.	Iceland
99.	India
100.	Indonesia
101.	Iran
102.	Iraq
103.	Ireland
104.	Isle of Man
105.	Israel
106.	Italy
107.	Ivory Coast
108.	Jamaica
109.	Japan
110.	Jersey
111.	Kazakhstan
112.	Kenya
113.	Kiribati
114.	Kosovo
115.	Kuwait
116.	Kyrgyzstan
117.	Laos
118.	Latvia
119.	Lebanon
120.	Lesotho
121.	Liberia
122.	Libya
123.	Liechtenstein
124.	Luxembourg
125.	Macao
126.	Macedonia

~~HIGHLY PROTECTED - ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

127.	Madagascar
128.	Malawi
129.	Malaysia
130.	Maldives
131.	Mali
132.	Malta
133.	Marshall Islands
134.	Martinique
135.	Mauritania
136.	Mauritius
137.	Mayotte
138.	Mexico
139.	Monaco
140.	Mongolia
141.	Montenegro
142.	Montserrat
143.	Morocco
144.	Mozambique
145.	Myanmar [Burma]
146.	Namibia
147.	Nauru
148.	Nepal
149.	Netherlands
150.	New Caledonia
151.	New Zealand
152.	Nicaragua
153.	Niger
154.	Nigeria
155.	Niue
156.	Norfolk Island
157.	North Korea
158.	Norway
159.	Oman
160.	Pakistan
161.	Palau
162.	Palestine
163.	Panama
164.	Papua New Guinea
165.	Paraguay
166.	Peru
167.	Philippines
168.	Pitcairn Islands
169.	Poland

~~HIGHLY PROTECTED - ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

170.	Portugal
171.	Qatar
172.	Republic of Korea
173.	Republic of Lithuania
174.	Republic of Moldova
175.	Republic of the Congo
176.	Romania
177.	Russia
178.	Rwanda
179.	Réunion
180.	Saint Helena
181.	Saint Kitts and Nevis
182.	Saint Lucia
183.	Saint Martin
184.	Saint Pierre and Miquelon
185.	Saint Vincent and the Grenadines
186.	Saint Barthélemy
187.	Samoa
188.	San Marino
189.	Saudi Arabia
190.	Senegal
191.	Serbia
192.	Seychelles
193.	Sierra Leone
194.	Singapore
195.	Sint Maarten
196.	Slovak Republic
197.	Slovakia
198.	Slovenia
199.	Solomon Islands
200.	Somalia
201.	South Africa
202.	South Georgia and the South Sandwich Islands
203.	South Sudan
204.	Spain
205.	Sri Lanka
206.	St Kitts and Nevis
207.	Sudan
208.	Suriname
209.	Svalbard and Jan Mayen
210.	Swaziland
211.	Sweden

~~HIGHLY PROTECTED - ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

212.	Switzerland
213.	Syria
214.	São Tomé and Príncipe
215.	Taiwan
216.	Tajikistan
217.	Tanzania
218.	Thailand
219.	Togo
220.	Tokelau
221.	Tonga
222.	Trinidad and Tobago
223.	Tunisia
224.	Turkey
225.	Turkmenistan
226.	Turks and Caicos Islands
227.	Tuvalu
228.	Uganda
229.	Ukraine
230.	United Arab Emirates
231.	United Kingdom
232.	Uruguay
233.	Uzbekistan
234.	Vanuatu
235.	Vatican City
236.	Venezuela
237.	Vietnam
238.	Wallis and Futuna
239.	Western Sahara
240.	Yemen
241.	Zambia
242.	Zimbabwe

EXHIBIT B

~~HIGHLY PROTECTED - ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

**List of Countries with HTTP Requests to Wikimedia
Servers in United States from August 1, 2017 to January 31, 2018**

1.	Afghanistan
2.	Åland
3.	Albania
4.	Algeria
5.	Andorra
6.	Angola
7.	Anguilla
8.	Antigua and Barbuda
9.	Argentina
10.	Armenia
11.	Aruba
12.	Australia
13.	Austria
14.	Azerbaijan
15.	Bahamas
16.	Bahrain
17.	Bangladesh
18.	Barbados
19.	Belarus
20.	Belgium
21.	Belize
22.	Benin
23.	Bermuda
24.	Bhutan
25.	Bolivia
26.	Bonaire, Sint Eustatius, and Saba
27.	Bosnia and Herzegovina
28.	Botswana
29.	Brazil
30.	British Indian Ocean Territory
31.	British Virgin Islands
32.	Brunei
33.	Bulgaria
34.	Burkina Faso
35.	Burundi
36.	Cabo Verde
37.	Cambodia
38.	Cameroon
39.	Canada
40.	Cayman Islands

~~HIGHLY PROTECTED - ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

41.	Central African Republic
42.	Chad
43.	Chile
44.	China
45.	Christmas Island
46.	Cocos [Keeling] Islands
47.	Colombia
48.	Comoros
49.	Congo
50.	Cook Islands
51.	Costa Rica
52.	Croatia
53.	Cuba
54.	Curaçao
55.	Cyprus
56.	Czechia
57.	Denmark
58.	Djibouti
59.	Dominica
60.	Dominican Republic
61.	East Timor
62.	Ecuador
63.	Egypt
64.	El Salvador
65.	Equatorial Guinea
66.	Eritrea
67.	Estonia
68.	Ethiopia
69.	Falkland Islands
70.	Faroe Islands
71.	Federated States of Micronesia
72.	Fiji
73.	Finland
74.	France
75.	French Guiana
76.	French Polynesia
77.	French Southern Territories
78.	Gabon
79.	Gambia
80.	Georgia
81.	Germany
82.	Ghana
83.	Gibraltar

~~HIGHLY PROTECTED - ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

84.	Greece
85.	Greenland
86.	Grenada
87.	Guadeloupe
88.	Guatemala
89.	Guernsey
90.	Guinea
91.	Guinea-Bissau
92.	Guyana
93.	Haiti
94.	Hashemite Kingdom of Jordan
95.	Honduras
96.	Hong Kong
97.	Hungary
98.	Iceland
99.	India
100.	Indonesia
101.	Iran
102.	Iraq
103.	Ireland
104.	Isle of Man
105.	Israel
106.	Italy
107.	Ivory Coast
108.	Jamaica
109.	Japan
110.	Jersey
111.	Kazakhstan
112.	Kenya
113.	Kiribati
114.	Kosovo
115.	Kuwait
116.	Kyrgyzstan
117.	Laos
118.	Latvia
119.	Lebanon
120.	Lesotho
121.	Liberia
122.	Libya
123.	Liechtenstein
124.	Luxembourg
125.	Macao
126.	Macedonia

~~HIGHLY PROTECTED - ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

127.	Madagascar
128.	Malawi
129.	Malaysia
130.	Maldives
131.	Mali
132.	Malta
133.	Marshall Islands
134.	Martinique
135.	Mauritania
136.	Mauritius
137.	Mayotte
138.	Mexico
139.	Monaco
140.	Mongolia
141.	Montenegro
142.	Montserrat
143.	Morocco
144.	Mozambique
145.	Myanmar [Burma]
146.	Namibia
147.	Nauru
148.	Nepal
149.	Netherlands
150.	New Caledonia
151.	New Zealand
152.	Nicaragua
153.	Niger
154.	Nigeria
155.	Niue
156.	Norfolk Island
157.	North Korea
158.	Norway
159.	Oman
160.	Pakistan
161.	Palau
162.	Palestine
163.	Panama
164.	Papua New Guinea
165.	Paraguay
166.	Peru
167.	Philippines
168.	Pitcairn Islands
169.	Poland

~~HIGHLY PROTECTED - ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

170.	Portugal
171.	Qatar
172.	Republic of Korea
173.	Republic of Lithuania
174.	Republic of Moldova
175.	Republic of the Congo
176.	Romania
177.	Russia
178.	Rwanda
179.	Réunion
180.	Saint Helena
181.	Saint Kitts and Nevis
182.	Saint Lucia
183.	Saint Martin
184.	Saint Pierre and Miquelon
185.	Saint Vincent and the Grenadines
186.	Saint Barthélemy
187.	Samoa
188.	San Marino
189.	Saudi Arabia
190.	Senegal
191.	Serbia
192.	Seychelles
193.	Sierra Leone
194.	Singapore
195.	Sint Maarten
196.	Slovak Republic
197.	Slovakia
198.	Slovenia
199.	Solomon Islands
200.	Somalia
201.	South Africa
202.	South Georgia and the South Sandwich Islands
203.	South Sudan
204.	Spain
205.	Sri Lanka
206.	St Kitts and Nevis
207.	Sudan
208.	Suriname
209.	Svalbard and Jan Mayen
210.	Swaziland
211.	Sweden

~~HIGHLY PROTECTED - ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

212.	Switzerland
213.	Syria
214.	São Tomé and Príncipe
215.	Taiwan
216.	Tajikistan
217.	Tanzania
218.	Thailand
219.	Togo
220.	Tokelau
221.	Tonga
222.	Trinidad and Tobago
223.	Tunisia
224.	Turkey
225.	Turkmenistan
226.	Turks and Caicos Islands
227.	Tuvalu
228.	Uganda
229.	Ukraine
230.	United Arab Emirates
231.	United Kingdom
232.	Uruguay
233.	Uzbekistan
234.	Vanuatu
235.	Vatican City
236.	Venezuela
237.	Vietnam
238.	Wallis and Futuna
239.	Western Sahara
240.	Yemen
241.	Zambia
242.	Zimbabwe

EXHIBIT C

~~HIGHLY PROTECTED - ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

List of Countries with Logged non-VPN TCP Connections to Wikimedia Office Router in United States from March 1, 2017 to February 28, 2018

1.	Andorra
2.	United Arab Emirates
3.	Afghanistan
4.	Antigua and Barbuda
5.	Albania
6.	Armenia
7.	Angola
8.	Antarctica
9.	Argentina
10.	Austria
11.	Australia
12.	Aruba
13.	Aland Islands
14.	Azerbaijan
15.	Bosnia and Herzegovina
16.	Barbados
17.	Bangladesh
18.	Belgium
19.	Burkina Faso
20.	Bulgaria
21.	Bahrain
22.	Burundi
23.	Benin
24.	Saint Bartelemey
25.	Bermuda
26.	Brunei Darussalam
27.	Bolivia
28.	Bonaire, Saint Eustatius and Saba
29.	Brazil
30.	Bahamas
31.	Bhutan
32.	Botswana
33.	Belarus
34.	Belize
35.	Canada
36.	Congo, The Democratic Republic of the
37.	Central African Republic
38.	Congo
39.	Switzerland
40.	Cote d'Ivoire

~~HIGHLY PROTECTED - ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

41.	Cook Islands
42.	Chile
43.	Cameroon
44.	China
45.	Colombia
46.	Costa Rica
47.	Cuba
48.	Cape Verde
49.	Curacao
50.	Christmas Island
51.	Cyprus
52.	Czech Republic
53.	Germany
54.	Djibouti
55.	Denmark
56.	Dominica
57.	Dominican Republic
58.	Algeria
59.	Ecuador
60.	Estonia
61.	Egypt
62.	Eritrea
63.	Spain
64.	Ethiopia
65.	Europe
66.	Finland
67.	Fiji
68.	France
69.	Gabon
70.	United Kingdom
71.	Grenada
72.	Georgia
73.	French Guiana
74.	Guernsey
75.	Ghana
76.	Gibraltar
77.	Greenland
78.	Gambia
79.	Guadeloupe
80.	Equatorial Guinea
81.	Greece
82.	Guatemala
83.	Guam

~~HIGHLY PROTECTED - ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

84.	Guyana
85.	Hong Kong
86.	Honduras
87.	Croatia
88.	Haiti
89.	Hungary
90.	Indonesia
91.	Ireland
92.	Israel
93.	Isle of Man
94.	India
95.	Iraq
96.	Iran, Islamic Republic of
97.	Iceland
98.	Italy
99.	Jersey
100.	Jamaica
101.	Jordan
102.	Japan
103.	Kenya
104.	Kyrgyzstan
105.	Cambodia
106.	Kiribati
107.	Comoros
108.	Saint Kitts and Nevis
109.	Korea, Democratic People's Republic of
110.	Korea, Republic of
111.	Kuwait
112.	Cayman Islands
113.	Kazakhstan
114.	Lao People's Democratic Republic
115.	Lebanon
116.	Saint Lucia
117.	Liechtenstein
118.	Sri Lanka
119.	Liberia
120.	Lesotho
121.	Lithuania
122.	Luxembourg
123.	Latvia
124.	Libyan Arab Jamahiriya
125.	Morocco
126.	Monaco

~~HIGHLY PROTECTED - ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

127.	Moldova, Republic of
128.	Montenegro
129.	Saint Martin
130.	Madagascar
131.	Marshall Islands
132.	Macedonia
133.	Mali
134.	Myanmar
135.	Mongolia
136.	Macao
137.	Northern Mariana Islands
138.	Martinique
139.	Mauritania
140.	Malta
141.	Mauritius
142.	Maldives
143.	Malawi
144.	Mexico
145.	Malaysia
146.	Mozambique
147.	Namibia
148.	New Caledonia
149.	Niger
150.	Nigeria
151.	Nicaragua
152.	Netherlands
153.	Norway
154.	Nepal
155.	New Zealand
156.	Oman
157.	Panama
158.	Peru
159.	French Polynesia
160.	Papua New Guinea
161.	Philippines
162.	Pakistan
163.	Poland
164.	Puerto Rico
165.	Palestinian Territory
166.	Portugal
167.	Palau
168.	Paraguay
169.	Qatar

~~HIGHLY PROTECTED - ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

170.	Reunion
171.	Romania
172.	Serbia
173.	Russian Federation
174.	Rwanda
175.	Saudi Arabia
176.	Solomon Islands
177.	Seychelles
178.	Sudan
179.	Sweden
180.	Singapore
181.	Slovenia
182.	Slovakia
183.	Sierra Leone
184.	Senegal
185.	Somalia
186.	Suriname
187.	South Sudan
188.	Sao Tome and Principe
189.	El Salvador
190.	Sint Maarten
191.	Syrian Arab Republic
192.	Swaziland
193.	Turks and Caicos Islands
194.	Chad
195.	Togo
196.	Thailand
197.	Tajikistan
198.	Turkmenistan
199.	Tunisia
200.	Tonga
201.	Turkey
202.	Trinidad and Tobago
203.	Taiwan
204.	Tanzania, United Republic of
205.	Ukraine
206.	Uganda
207.	Uruguay
208.	Uzbekistan
209.	Holy See (Vatican City State)
210.	Saint Vincent and the Grenadines
211.	Venezuela
212.	Virgin Islands, British

~~HIGHLY PROTECTED - ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

213.	Virgin Islands, U.S.
214.	Vietnam
215.	Vanuatu
216.	Samoa
217.	Kosovo
218.	Yemen
219.	South Africa
220.	Zambia
221.	Zimbabwe

EXHIBIT D

~~HIGHLY PROTECTED - ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

**List of Countries with Logged VPN TCP Connections to Wikimedia
Office Router in United States from March 1, 2017 to February 28, 2018**

1.	United Arab Emirates
2.	Bulgaria
3.	Brazil
4.	Canada
5.	Switzerland
6.	China
7.	Colombia
8.	Germany
9.	Spain
10.	France
11.	United Kingdom
12.	Greece
13.	Hong Kong
14.	Ireland
15.	Iceland
16.	Japan
17.	Korea, Republic of
18.	Latvia
19.	Moldova, Republic of
20.	Mongolia
21.	Nigeria
22.	Netherlands
23.	Portugal
24.	Romania
25.	Russian Federation
26.	Seychelles
27.	Singapore
28.	Ukraine
29.	Uzbekistan

EXHIBIT E

~~HIGHLY PROTECTED - ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

List of Countries with Logged non-VPN UDP Connections to Wikimedia Office Router in United States from March 1, 2017 to February 28, 2018

1.	United Arab Emirates
2.	Antigua and Barbuda
3.	Anguilla
4.	Albania
5.	Armenia
6.	Angola
7.	Antarctica
8.	Argentina
9.	Austria
10.	Australia
11.	Aruba
12.	Aland Islands
13.	Azerbaijan
14.	Bosnia and Herzegovina
15.	Barbados
16.	Bangladesh
17.	Belgium
18.	Burkina Faso
19.	Bulgaria
20.	Bahrain
21.	Burundi
22.	Benin
23.	Bermuda
24.	Brunei Darussalam
25.	Bolivia
26.	Bonaire, Saint Eustatius and Saba
27.	Brazil
28.	Bahamas
29.	Bhutan
30.	Botswana
31.	Belarus
32.	Belize
33.	Canada
34.	Switzerland
35.	Cote d'Ivoire
36.	Cook Islands
37.	Chile
38.	Cameroon
39.	China
40.	Colombia

~~HIGHLY PROTECTED - ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

41.	Costa Rica
42.	Cuba
43.	Cape Verde
44.	Curacao
45.	Cyprus
46.	Czech Republic
47.	Germany
48.	Denmark
49.	Dominica
50.	Dominican Republic
51.	Algeria
52.	Ecuador
53.	Estonia
54.	Egypt
55.	Spain
56.	Ethiopia
57.	Europe
58.	Finland
59.	Fiji
60.	France
61.	Gabon
62.	United Kingdom
63.	Grenada
64.	Georgia
65.	French Guiana
66.	Guernsey
67.	Ghana
68.	Gibraltar
69.	Greenland
70.	Guinea
71.	Guadeloupe
72.	Greece
73.	Guatemala
74.	Guam
75.	Guyana
76.	Hong Kong
77.	Honduras
78.	Croatia
79.	Hungary
80.	Indonesia
81.	Ireland
82.	Israel
83.	Isle of Man

~~HIGHLY PROTECTED - ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

84.	India
85.	Iraq
86.	Iran, Islamic Republic of
87.	Iceland
88.	Italy
89.	Jersey
90.	Jamaica
91.	Jordan
92.	Japan
93.	Kenya
94.	Kyrgyzstan
95.	Cambodia
96.	Comoros
97.	Saint Kitts and Nevis
98.	Korea, Democratic People's Republic of
99.	Korea, Republic of
100.	Kuwait
101.	Cayman Islands
102.	Kazakhstan
103.	Lao People's Democratic Republic
104.	Lebanon
105.	Saint Lucia
106.	Liechtenstein
107.	Sri Lanka
108.	Lithuania
109.	Luxembourg
110.	Latvia
111.	Libyan Arab Jamahiriya
112.	Morocco
113.	Monaco
114.	Moldova, Republic of
115.	Montenegro
116.	Saint Martin
117.	Madagascar
118.	Macedonia
119.	Myanmar
120.	Mongolia
121.	Macao
122.	Martinique
123.	Mauritania
124.	Montserrat
125.	Malta
126.	Mauritius

~~HIGHLY PROTECTED - ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

127.	Maldives
128.	Malawi
129.	Mexico
130.	Malaysia
131.	Mozambique
132.	Namibia
133.	New Caledonia
134.	Niger
135.	Nigeria
136.	Nicaragua
137.	Netherlands
138.	Norway
139.	Nepal
140.	Nauru
141.	New Zealand
142.	Oman
143.	Panama
144.	Peru
145.	French Polynesia
146.	Philippines
147.	Pakistan
148.	Poland
149.	Puerto Rico
150.	Palestinian Territory
151.	Portugal
152.	Paraguay
153.	Qatar
154.	Reunion
155.	Romania
156.	Serbia
157.	Russian Federation
158.	Rwanda
159.	Saudi Arabia
160.	Seychelles
161.	Sudan
162.	Sweden
163.	Singapore
164.	Slovenia
165.	Slovakia
166.	Sierra Leone
167.	San Marino
168.	Senegal
169.	Somalia

~~HIGHLY PROTECTED - ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

170.	Suriname
171.	El Salvador
172.	Sint Maarten
173.	Syrian Arab Republic
174.	Swaziland
175.	Turks and Caicos Islands
176.	Chad
177.	Togo
178.	Thailand
179.	Tajikistan
180.	Tokelau
181.	Turkmenistan
182.	Tunisia
183.	Turkey
184.	Trinidad and Tobago
185.	Taiwan
186.	Tanzania, United Republic of
187.	Ukraine
188.	Uganda
189.	Uruguay
190.	Uzbekistan
191.	Holy See (Vatican City State)
192.	Saint Vincent and the Grenadines
193.	Venezuela
194.	Virgin Islands, British
195.	Virgin Islands, U.S.
196.	Vietnam
197.	Vanuatu
198.	Kosovo
199.	Yemen
200.	Mayotte
201.	South Africa
202.	Zambia
203.	Zimbabwe

EXHIBIT F

~~HIGHLY PROTECTED - ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

**List of Countries with Logged VPN UDP Connections to Wikimedia
Office Router in United States from March 1, 2017 to February 28, 2018**

1.	Argentina
2.	Austria
3.	Australia
4.	Canada
5.	China
6.	Colombia
7.	Czech Republic
8.	Germany
9.	Denmark
10.	Egypt
11.	Spain
12.	France
13.	United Kingdom
14.	Greece
15.	Hungary
16.	Iran, Islamic Republic of
17.	Jordan
18.	Mexico
19.	Netherlands
20.	New Zealand
21.	Peru
22.	Poland
23.	Russian Federation
24.	Seychelles
25.	Sweden
26.	Turkey
27.	Uzbekistan

EXHIBIT G

~~HIGHLY PROTECTED - ATTORNEYS EYES ONLY~~
~~FOIA Confidential Treatment Request~~

List of Countries with Logged non-VPN ICMP Connections to Wikimedia Office Router in United States from August 1, 2017 to January 31, 2018

1.	United Arab Emirates
2.	Albania
3.	Armenia
4.	Argentina
5.	Austria
6.	Australia
7.	Azerbaijan
8.	Bosnia and Herzegovina
9.	Bangladesh
10.	Belgium
11.	Bulgaria
12.	Bolivia
13.	Brazil
14.	Belarus
15.	Canada
16.	Switzerland
17.	Chile
18.	China
19.	Colombia
20.	Costa Rica
21.	Czech Republic
22.	Germany
23.	Denmark
24.	Dominican Republic
25.	Ecuador
26.	Estonia
27.	Egypt
28.	Spain
29.	Europe
30.	Finland
31.	France
32.	United Kingdom
33.	Georgia
34.	Ghana
35.	Greece
36.	Guatemala
37.	Hong Kong
38.	Croatia
39.	Hungary
40.	Indonesia

~~HIGHLY PROTECTED - ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

41.	Ireland
42.	Israel
43.	India
44.	Iran, Islamic Republic of
45.	Iceland
46.	Italy
47.	Jordan
48.	Japan
49.	Kenya
50.	Kyrgyzstan
51.	Cambodia
52.	Korea, Republic of
53.	Kuwait
54.	Kazakhstan
55.	Lao People's Democratic Republic
56.	Lebanon
57.	Sri Lanka
58.	Lithuania
59.	Luxembourg
60.	Latvia
61.	Morocco
62.	Moldova, Republic of
63.	Macedonia
64.	Mongolia
65.	Mauritius
66.	Mexico
67.	Malaysia
68.	Mozambique
69.	New Caledonia
70.	Netherlands
71.	Norway
72.	Nepal
73.	New Zealand
74.	Peru
75.	French Polynesia
76.	Philippines
77.	Pakistan
78.	Poland
79.	Portugal
80.	Romania
81.	Serbia
82.	Russian Federation
83.	Rwanda

~~HIGHLY PROTECTED - ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

84.	Saudi Arabia
85.	Seychelles
86.	Sudan
87.	Sweden
88.	Singapore
89.	Slovenia
90.	Slovakia
91.	El Salvador
92.	Thailand
93.	Tunisia
94.	Turkey
95.	Taiwan
96.	Tanzania, United Republic of
97.	Ukraine
98.	Uruguay
99.	Uzbekistan
100.	Venezuela
101.	Vietnam
102.	Vanuatu
103.	Kosovo
104.	South Africa
105.	Zimbabwe

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 15

We the People

Article I

Privacy and Civil Liberties Oversight Board

Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act

JULY 2, 2014





PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

***Report on the Surveillance Program Operated Pursuant to Section 702
of the Foreign Intelligence Surveillance Act***

JULY 2, 2014

Privacy and Civil Liberties Oversight Board

David Medine, Chairman

Rachel Brand

Elisebeth Collins Cook

James Dempsey

Patricia Wald



PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

**Report on the Surveillance Program Operated Pursuant to Section 702
of the Foreign Intelligence Surveillance Act**

Part 1 INTRODUCTION 1

Part 2 EXECUTIVE SUMMARY..... 5

Part 3 DESCRIPTION AND HISTORY 16

 Genesis of the Section 702 Program 16

 Statutory Structure 20

 Acquisition Process 32

 Targeting Procedures 41

 Post-Tasking Review 48

 Minimization Procedures 50

 Internal Agency Oversight 66

 External Oversight 70

 Compliance Issues 77

Part 4 LEGAL ANALYSIS 80

 Statutory Analysis 80

 Constitutional Analysis 86

Analysis of Treatment of Non-U.S. Persons	98
Part 5 POLICY ANALYSIS	103
Value of the Section 702 Program	104
Privacy and Civil Liberties Implications of the Section 702 Program	111
Part 6 RECOMMENDATIONS	134
Part 7 CONCLUSION	149
ANNEXES.....	150
A. Separate Statement by Chairman David Medine and Board Member Patricia Wald	151
B. Separate Statement by Board Members Rachel Brand and Elisebeth Collins Cook	161
C. July 9, 2013 Workshop Agenda and Link to Workshop Transcript	166
D. November 4, 2013 Hearing Agenda and Link to Hearing Transcript.....	169
E. March 19, 2014 Hearing Agenda and Link to Hearing Transcript	172
F. Request for Public Comments on Board Study	175
G. Reopening the Public Comment Period	177
H. Index to Public Comments on www.regulations.gov	178

Part 1:

INTRODUCTION

I. Background

Shortly after the Privacy and Civil Liberties Oversight Board (“PCLOB” or “Board”) began operation as a new independent agency, Board Members identified a series of programs and issues to prioritize for review. As announced at the Board’s public meeting in March 2013, one of these issues was the implementation of the Foreign Intelligence Surveillance Act Amendments Act of 2008.¹

Several months later, in June 2013, two classified National Security Agency (“NSA”) collection programs were first reported about by the press based on unauthorized disclosures of classified documents by Edward Snowden, a contractor for the NSA. Under one program, implemented under Section 215 of the USA PATRIOT Act, the NSA collects domestic telephone metadata (i.e., call records) in bulk. Under the other program, implemented under Section 702 of the Foreign Intelligence Surveillance Act (“FISA”), the government collects the contents of electronic communications, including telephone calls and emails, where the target is reasonably believed to be a non-U.S. person² located outside the United States.

A bipartisan group of U.S. Senators asked the Board to investigate the two NSA programs and provide an unclassified report.³ House Minority Leader Nancy Pelosi subsequently asked the Board to consider the operations of the Foreign Intelligence Surveillance Court (“FISA court”).⁴ Additionally, the Board met with President Obama, who asked the Board to “review where our counterterrorism efforts and our values come into

¹ See Privacy and Civil Liberties Oversight Board, Minutes of Open Meeting of March 5, 2013, at 4-5, available at <http://www.pclob.gov/SiteAssets/meetings-and-events/5-march-2013-public-meeting/5%20March%202013%20Meeting%20Minutes.pdf>.

² Under the statute, the term “U.S. persons” includes United States citizens, United States permanent residents, and virtually all United States corporations.

³ Letter from Tom Udall *et al.* to the Privacy and Civil Liberties Oversight Board (June 12, 2013), available at <http://www.pclob.gov/SiteAssets/newsroom/6.12.13%20Senate%20letter%20to%20PCLOB.pdf>. Response available at http://www.pclob.gov/SiteAssets/newsroom/PCLOB_TUdall.pdf.

⁴ Letter from Democratic Leader Nancy Pelosi to Chairman David Medine (July 11, 2013), available at <http://www.pclob.gov/SiteAssets/newsroom/Pelosi%20Letter%20to%20PCLOB.pdf>. Response available at <http://www.pclob.gov/SiteAssets/newsroom/PCLOB%20Pelosi%20Response%20Final.pdf>.

tension.”⁵ In response to the requests from Congress and the President, the Board began a comprehensive study of the two NSA programs. The Board held public hearings and met with the Intelligence Community and the Department of Justice, White House, and congressional committee staff, privacy and civil liberties advocates, academics, trade associations, and technology and communications companies.

During the course of this study, it became clear to the Board that each program required a level of review that was best undertaken and presented to the public in a separate report. As such, the Board released a report on the Section 215 telephone records program and the operation of the FISA court on January 23, 2014.⁶ Subsequently, the Board held an additional public hearing and continued its study of the second program. Now, the Board is issuing the current report, which examines the collection of electronic communications under Section 702, and provides analysis and recommendations regarding the program’s implementation.

The Section 702 program is extremely complex, involving multiple agencies, collecting multiple types of information, for multiple purposes. Overall, the Board has found that the information the program collects has been valuable and effective in protecting the nation’s security and producing useful foreign intelligence. The program has operated under a statute that was publicly debated, and the text of the statute outlines the basic structure of the program. Operation of the Section 702 program has been subject to judicial oversight and extensive internal supervision, and the Board has found no evidence of intentional abuse.

The Board has found that certain aspects of the program’s implementation raise privacy concerns. These include the scope of the incidental collection of U.S. persons’ communications and the use of queries to search the information collected under the program for the communications of specific U.S. persons. The Board offers a series of policy recommendations to strengthen privacy safeguards and to address these concerns.

II. Study Methodology

In order to gain a full understanding of the program’s operations, the Board and its staff received multiple briefings on the operation of the program, including the technical

⁵ Remarks by the President in a Press Conference at the White House (Aug. 9, 2013), *available at* <http://www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference>.

⁶ See PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (2014), *available at* <http://www.pclob.gov/All%20Documents/Report%20on%20the%20Telephone%20Records%20Program/PCLOB-Report-on-the-Telephone-Records-Program.pdf>.

details and procedural rules that govern its implementation. The Board appreciates the responsiveness and open lines of communication that have been established with members of the Intelligence Community and the Department of Justice. These have enabled the Board to understand the operation of this complex program, and to fully consider the practical impact that the Board's recommendations will have.

Building upon the previous public hearings held in July and November 2013, the Board held an additional public hearing on March 19, 2014, focused exclusively on the Section 702 program.⁷ This hearing was comprised of three panels. The first panel consisted of government representatives who provided the government's views on Section 702. The second panel consisted of academics and privacy advocates who addressed the legal issues related to Section 702, including both statutory and constitutional matters. The third panel consisted of representatives from private industry, academics, and human rights organizations who discussed the transnational and policy issues related to Section 702. Panelists, as well as the general public, were invited to submit written comments to the Board via www.regulations.gov.⁸

Since the unauthorized disclosures that began in 2013, much of the information that the Intelligence Community has declassified and released has related to the Section 215 program. In the preparation of this Report, the Board worked with the Intelligence Community to seek further declassification of information related to the Section 702 program. Specifically, the Board requested declassification of additional facts for use in this Report. Consistent with the Board's goal of seeking greater transparency where appropriate, the request for declassification of additional facts to be used in this Report was made in order to provide further clarity and education to the public about the Section 702 program. The Intelligence Community carefully considered the Board's requests and has engaged in a productive dialogue with PCLOB staff. The Board greatly appreciates the diligent efforts of the Intelligence Community to work through the declassification process, and as a result of the process, many facts that were previously classified are now available to the public.

In the course of preparing and finalizing this Report, the Board met with staff from the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, as well as staff from the House and Senate Judiciary Committees, to discuss the Section 702 program and the Board's preliminary recommendations. The Board also presented its preliminary recommendations to senior staff at the White House. In addition, the Board provided a draft of this Report to the Intelligence Community for classification review. While the Board's report was subject to classification review, and while the Board

⁷ See Annex E.

⁸ See Annex H.

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.

III. Report Organization

This Report consists of six parts. After this introduction and the Executive Summary, Part 3 contains a factual narrative that explains the development of the Section 702 program and how the program currently operates. Part 4 consists of legal analysis, including the Board's statutory and constitutional analyses, as well as a discussion of how the program affects the legal rights of non-U.S. persons. Part 5 examines the policy implications of the program, including an assessment of its efficacy and its effect on privacy, while Part 6 outlines and explains the Board's recommendations.

The Board presents this Report in an effort to provide greater transparency and clarity to the public regarding the government's activities with respect to the Section 702 program. The recommendations reflect the Board's best efforts to protect the privacy and civil liberties of the public while considering legitimate national security interests. The Board welcomes the opportunity for further discussion of these pressing issues.

Part 2:

EXECUTIVE SUMMARY

In 2008, Congress enacted the FISA Amendments Act, which made changes to the Foreign Intelligence Surveillance Act of 1978 (“FISA”). Among those changes was the addition of a new provision, Section 702 of FISA, permitting the Attorney General and the Director of National Intelligence to jointly authorize surveillance conducted within the United States but targeting only non-U.S. persons reasonably believed to be located outside the United States. The Privacy and Civil Liberties Oversight Board (“PCLOB”) began reviewing implementation of the FISA Amendments Act early in 2013, shortly after the Board began operations as an independent agency.⁹ The PCLOB has conducted an in-depth review of the program now operated under Section 702, in pursuit of the Board’s mission to review executive branch actions taken to protect the nation from terrorism in order to ensure “that the need for such actions is balanced with the need to protect privacy and civil liberties.”¹⁰ This Executive Summary outlines the Board’s conclusions and recommendations.

I. Overview of the Report

A. Description and History of the Section 702 Program

Section 702 has its roots in the President’s Surveillance Program developed in the immediate aftermath of the September 11th attacks. Under one aspect of that program, which came to be known as the Terrorist Surveillance Program (“TSP”), the President authorized interception of the contents of international communications from within the United States, outside of the FISA process. Following disclosures about the TSP by the press in December 2005, the government sought and obtained authorization from the Foreign Intelligence Surveillance Court (“FISA court”) to conduct, under FISA, the collection that had been occurring under the TSP. Later, the government developed a statutory framework specifically designed to authorize this collection program. After the enactment and expiration of a temporary measure, the Protect America Act of 2007, Congress passed the FISA Amendments Act of 2008, which included the new Section 702 of FISA. The statute

⁹ See Privacy and Civil Liberties Oversight Board, Minutes of Open Meeting of March 5, 2013, at 4-5, available at <http://www.pclob.gov/SiteAssets/meetings-and-events/5-march-2013-public-meeting/5%20March%202013%20Meeting%20Minutes.pdf>.

¹⁰ 42 U.S.C. § 2000ee(c)(1).

provides a procedural framework for the targeting of non-U.S. persons reasonably believed to be located outside the United States to acquire foreign intelligence information.

Section 702 permits the Attorney General and the Director of National Intelligence to jointly authorize surveillance targeting persons who are not U.S. persons, and who are reasonably believed to be located outside the United States, with the compelled assistance of electronic communication service providers, in order to acquire foreign intelligence information. Thus, the persons who may be targeted under Section 702 cannot intentionally include U.S. persons or anyone located in the United States, and the targeting must be conducted to acquire foreign intelligence information as defined in FISA. Executive branch authorizations to acquire designated types of foreign intelligence under Section 702 must be approved by the FISA court, along with procedures governing targeting decisions and the handling of information acquired.

Although U.S. persons may not be targeted under Section 702, communications of or concerning U.S. persons may be acquired in a variety of ways. An example is when a U.S. person communicates with a non-U.S. person who has been targeted, resulting in what is termed “incidental” collection. Another example is when two non-U.S. persons discuss a U.S. person. Communications of or concerning U.S. persons that are acquired in these ways may be retained and used by the government, subject to applicable rules and requirements. The communications of U.S. persons may also be collected by mistake, as when a U.S. person is erroneously targeted or in the event of a technological malfunction, resulting in “inadvertent” collection. In such cases, however, the applicable rules generally require the communications to be destroyed.

Under Section 702, the Attorney General and Director of National Intelligence make annual certifications authorizing this targeting to acquire foreign intelligence information, without specifying to the FISA court the particular non-U.S. persons who will be targeted. There is no requirement that the government demonstrate probable cause to believe that an individual targeted is an agent of a foreign power, as is generally required in the “traditional” FISA process under Title I of the statute. Instead, the Section 702 certifications identify categories of information to be collected, which must meet the statutory definition of foreign intelligence information. The certifications that have been authorized include information concerning international terrorism and other topics, such as the acquisition of weapons of mass destruction.

Section 702 requires the government to develop targeting and “minimization” procedures that must satisfy certain criteria. As part of the FISA court’s review and approval of the government’s annual certifications, the court must approve these procedures and determine that they meet the necessary standards. The targeting procedures govern how the executive branch determines that a particular person is reasonably believed to be a non-U.S. person located outside the United States, and that

targeting this person will lead to the acquisition of foreign intelligence information. The minimization procedures cover the acquisition, retention, use, and dissemination of any non-publicly available U.S. person information acquired through the Section 702 program.

Once foreign intelligence acquisition has been authorized under Section 702, the government sends written directives to electronic communication service providers compelling their assistance in the acquisition of communications. The government identifies or “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. There are two types of Section 702 acquisition: what has been referred to as “PRISM” collection and “upstream” collection.

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.

Upstream collection differs from PRISM collection in several respects. First, the acquisition 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. Upstream collection also includes telephone calls in addition to Internet communications. Data from upstream collection is received only by the NSA: neither the CIA nor the FBI has access to unminimized upstream data. Finally, the upstream collection of Internet communications includes two features that are not present in PRISM collection: the acquisition of so-called “about” communications and the acquisition of so-called “multiple communications transactions” (“MCTs”). 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. 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.

Each agency that receives communications under Section 702 has its own minimization procedures, approved by the FISA court, that govern the agency’s use,

retention, and dissemination of Section 702 data.¹¹ Among other things, these procedures include rules on how the agencies may “query” the collected data. The NSA, CIA, and FBI minimization procedures all include provisions permitting these agencies to query data acquired through Section 702, using terms intended to discover or retrieve communications content or metadata that meets the criteria specified in the query. These queries may include terms that identify specific U.S. persons and can be used to retrieve the already acquired communications of specific U.S. persons. Minimization procedures set forth the standards for conducting queries. For example, the NSA’s minimization procedures require that queries of Section 702–acquired information be designed so that they are “reasonably likely to return foreign intelligence information.”

The minimization procedures also include data retention limits and rules outlining circumstances under which information must be purged. Apart from communications acquired by mistake, U.S. persons’ communications are not typically purged or eliminated from agency databases, even when they do not contain foreign intelligence information, until the data is aged off in accordance with retention limits.

Each agency’s adherence to its targeting and minimization procedures is subject to extensive oversight within the executive branch, including internal oversight within individual agencies as well as regular reviews conducted by the Department of Justice (“DOJ”) and the Office of the Director of National Intelligence (“ODNI”). The Section 702 program is also subject to oversight by the FISA court, including during the annual certification process and when compliance incidents are reported to the court. Information about the operation of the program also is reported to congressional committees. Although there have been various compliance incidents over the years, many of these incidents have involved technical issues resulting from the complexity of the program, and the Board has not seen any evidence of bad faith or misconduct.

B. Legal Analysis

The Board’s legal analysis of the Section 702 program includes an evaluation of whether it comports with the terms of the statute, an evaluation of the Fourth Amendment issues raised by the program, and a discussion of the treatment of non-U.S. persons under the program.

In reviewing the program’s compliance with the text of Section 702, the Board has assessed the operation of the program overall and has separately evaluated PRISM and upstream collection. On the whole, the text of Section 702 provides the public with transparency into the legal framework for collection, and it publicly outlines the basic

¹¹ As described in Part 3 of this Report, the National Counterterrorism Center (“NCTC”) has some access to Section 702 data and therefore has its own minimization procedures as well. However, the NCTC’s role in processing and minimizing Section 702 data is limited.

structure of the program. The Board concludes that PRISM collection is clearly authorized by the statute and that, with respect to the “about” collection, which occurs in the upstream component of the program, the statute can permissibly be interpreted as allowing such collection as it is currently implemented.

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 communicate foreign intelligence, using specific communications identifiers, subject to FISA court–approved targeting rules and multiple layers of oversight — fits within the “totality of the circumstances” standard for reasonableness under the Fourth Amendment, as that standard has been defined by the courts to date. Outside of this fundamental core, certain aspects of the Section 702 program push the program close to the line of constitutional reasonableness. Such aspects include the unknown and potentially large scope of the incidental collection of U.S. persons’ communications, the use of “about” collection to acquire Internet communications that are neither to nor from the target of surveillance, and the use of queries to search for the communications of specific U.S. persons within the information that has been collected. With these concerns in mind, this Report offers a set of policy proposals designed to push the program more comfortably into the sphere of reasonableness, ensuring that the program remains tied to its constitutionally legitimate core.

Finally, the Board discusses the fact that privacy is a human right that has been recognized in the International Covenant on Civil and Political Rights (“ICCPR”), an international treaty ratified by the U.S. Senate, and that the treatment of non-U.S. persons in U.S. surveillance programs raises important but difficult legal and policy questions. Many of the generally applicable protections that already exist under U.S. surveillance laws apply to U.S. and non-U.S. persons alike. The President’s recent initiative under Presidential Policy Directive 28 on Signals Intelligence (“PPD-28”) will further address the extent to which non-U.S. persons should be afforded the same protections as U.S. persons under U.S. surveillance laws.¹² Because PPD-28 invites the PCLOB to be involved in its implementation, the Board has concluded that it can make its most productive contribution in assessing these issues in the context of the PPD-28 review process.

C. Policy Analysis

The Section 702 program has enabled the government to acquire a greater range of foreign intelligence than it otherwise would have been able to obtain — and to do so quickly and effectively. Compared with the “traditional” FISA process under Title I of the

¹² See Presidential Policy Directive — Signals Intelligence Activities, Policy Directive 28, 2014 WL 187435 (Jan. 17, 2014) (“PPD-28”), available at <http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>.

statute, Section 702 imposes significantly fewer limits on the government when it targets foreigners located abroad, permitting greater flexibility and a dramatic increase in the number of people who can realistically be targeted. The program has proven valuable in the government's efforts to combat terrorism as well as in other areas of foreign intelligence. Presently, over a quarter of the NSA's reports concerning international terrorism include information based in whole or in part on Section 702 collection, and this percentage has increased every year since the statute was enacted. Monitoring terrorist networks under Section 702 has enabled the government to learn how they operate, and to understand their priorities, strategies, and tactics. In addition, the program has led the government to identify previously unknown individuals who are involved in international terrorism, and it has played a key role in discovering and disrupting specific terrorist plots aimed at the United States and other countries.

The basic structure of the Section 702 program appropriately focuses on targeting non-U.S. persons reasonably believed to be located abroad. Yet communications of, or concerning, U.S. persons can be collected under Section 702, and certain features of the program implicate privacy concerns. These features include the potential scope of U.S. person communications that are collected, the acquisition of "about" communications, and the use of queries that employ U.S. person identifiers.

The Board's analysis of these features of the program leads to certain policy recommendations.

The government is presently unable to assess the scope of the incidental collection of U.S. person information under the program. For this reason, the Board recommends several measures that together may provide insight about the extent to which communications involving U.S. persons or people located in the United States are being acquired and utilized.

With regard to the NSA's acquisition of "about" communications, the Board concludes that the practice is largely an inevitable byproduct of the government's efforts to comprehensively acquire communications that are sent to or from its targets. Because of the manner in which the NSA conducts upstream collection, and the limits of its current technology, the NSA cannot completely eliminate "about" communications from its collection without also eliminating a significant portion of the "to/from" communications that it seeks. The Board includes a recommendation to better assess "about" collection and a recommendation to ensure that upstream collection as a whole does not unnecessarily collect domestic communications.

The Report also assesses the impact of queries using "United States person identifiers." At the NSA, for example, these queries can be performed if they are deemed "reasonably likely to return foreign intelligence information." No showing of suspicion that

the U.S. person is engaged in any form of wrongdoing is required, but procedures are in place to prevent queries being conducted for improper purposes. The Board includes two recommendations to address the rules regarding U.S. person queries.

Overall, the Board finds that the protections contained in the Section 702 minimization procedures are reasonably designed and implemented to ward against the exploitation of information acquired under the program for illegitimate purposes. The Board has seen no trace of any such illegitimate activity associated with the program, or any attempt to intentionally circumvent legal limits. But the applicable rules potentially allow a great deal of private information about U.S. persons to be acquired by the government. The Board therefore offers a series of policy recommendations to ensure that the program appropriately balances national security with privacy and civil liberties.

II. Recommendations

A. Targeting and Tasking

Recommendation 1: *The NSA's targeting procedures should be revised to (a) specify criteria for determining the expected foreign intelligence value of a particular target, and (b) require a written explanation of the basis for that determination sufficient to demonstrate that the targeting of each selector is likely to return foreign intelligence information relevant to the subject of one of the certifications approved by the FISA court. The NSA should implement these revised targeting procedures through revised guidance and training for analysts, specifying the criteria for the foreign intelligence determination and the kind of written explanation needed to support it. We expect that the FISA court's review of these targeting procedures in the course of the court's periodic review of Section 702 certifications will include an assessment of whether the revised procedures provide adequate guidance to ensure that targeting decisions are reasonably designed to acquire foreign intelligence information relevant to the subject of one of the certifications approved by the FISA court. Upon revision of the NSA's targeting procedures, internal agency reviews, as well as compliance audits performed by the ODNI and DOJ, should include an assessment of compliance with the foreign intelligence purpose requirement comparable to the review currently conducted of compliance with the requirement that targets are reasonably believed to be non-U.S. persons located outside the United States.*

B. U.S. Person Queries

Recommendation 2: *The FBI's minimization procedures should be updated to more clearly reflect the actual practice for conducting U.S. person queries, including the frequency with which Section 702 data may be searched when making routine queries as part of FBI*

assessments and investigations. Further, some additional limits should be placed on the FBI's use and dissemination of Section 702 data in connection with non-foreign intelligence criminal matters.

Recommendation 3: *The NSA and CIA minimization procedures should permit the agencies to query collected Section 702 data for foreign intelligence purposes using U.S. person identifiers only if the query is based upon a statement of facts showing that it is reasonably likely to return foreign intelligence information as defined in FISA. The NSA and CIA should develop written guidance for agents and analysts as to what information and documentation is needed to meet this standard, including specific examples.*

C. FISA Court Role

Recommendation 4: *To assist in the FISA court's consideration of the government's periodic Section 702 certification applications, the government should submit with those applications a random sample of tasking sheets and a random sample of the NSA's and CIA's U.S. person query terms, with supporting documentation. The sample size and methodology should be approved by the FISA court.*

Recommendation 5: *As part of the periodic certification process, the government should incorporate into its submission to the FISA court the rules for operation of the Section 702 program that have not already been included in certification orders by the FISA court, and that at present are contained in separate orders and opinions, affidavits, compliance and other letters, hearing transcripts, and mandatory reports filed by the government. To the extent that the FISA court agrees that these rules govern the operation of the Section 702 program, the FISA court should expressly incorporate them into its order approving Section 702 certifications.*

D. Upstream and "About" Collection

Recommendation 6: *To build on current efforts to filter upstream communications to avoid collection of purely domestic communications, the NSA and DOJ, in consultation with affected telecommunications service providers, and as appropriate, with independent experts, should periodically assess whether filtering techniques applied in upstream collection utilize the best technology consistent with program needs to ensure government acquisition of only communications that are authorized for collection and prevent the inadvertent collection of domestic communications.*

Recommendation 7: *The NSA periodically should review the types of communications acquired through “about” collection under Section 702, and study the extent to which it would be technically feasible to limit, as appropriate, the types of “about” collection.*

E. Accountability and Transparency

Recommendation 8: *To the maximum extent consistent with national security, the government should create and release, with minimal redactions, declassified versions of the FBI’s and CIA’s Section 702 minimization procedures, as well as the NSA’s current minimization procedures.*

Recommendation 9: *The government should implement five measures to provide insight about the extent to which the NSA acquires and utilizes the communications involving U.S. persons and people located in the United States under the Section 702 program. Specifically, the NSA should implement processes to annually count the following: (1) the number of telephone communications acquired in which one caller is located in the United States; (2) the number of Internet communications acquired through upstream collection that originate or terminate in the United States; (3) the number of communications of or concerning U.S. persons that the NSA positively identifies as such in the routine course of its work; (4) the number of queries performed that employ U.S. person identifiers, specifically distinguishing the number of such queries that include names, titles, or other identifiers potentially associated with individuals; and (5) the number of instances in which the NSA disseminates non-public information about U.S. persons, specifically distinguishing disseminations that includes names, titles, or other identifiers potentially associated with individuals. These figures should be reported to Congress in the NSA Director’s annual report and should be released publicly to the extent consistent with national security.*

F. Efficacy

Recommendation 10: *The government should develop a comprehensive methodology for assessing the efficacy and relative value of counterterrorism programs.*

III. Separate Statements

Following the Board's recommendations, the Report includes two separate statements.

A. Separate Statement of Chairman David Medine and Board Member Patricia Wald

Chairman David Medine and Member Patricia Wald wrote jointly to recommend requiring restrictions additional to those contained in Recommendation 3 with regard to U.S. person queries conducted for a foreign intelligence purpose. They also recommended that minimization procedures governing the use of U.S. persons' communications collected under Section 702 should require the following:

(1) No later than when the results of a U.S. person query of Section 702 data are generated, U.S. persons' communications should be purged of information that does not meet the statutory definition of foreign intelligence information relating to U.S. persons.¹³ This process should be subject to judicial oversight.¹⁴

(2) Each U.S. person identifier should be submitted to the FISA court for approval before the identifier may be used to query data collected under Section 702, for a foreign intelligence purpose, other than in exigent circumstances or where otherwise required by law. The FISA court should determine, based on documentation submitted by the government, whether the use of the U.S. person identifier for Section 702 queries meets the standard that the identifier is reasonably likely to return foreign intelligence information as defined under FISA.¹⁵

In addition, they wrote to further explain their views regarding Recommendation 2. Specifically, they believe that the additional limits to be placed on the FBI's use and dissemination of Section 702 data in connection with non-foreign intelligence criminal matters should include the requirement that the FBI obtain prior FISA court approval before using identifiers to query Section 702 data to ensure that the identifier is reasonably likely to return information relevant to an assessment or investigation of a crime.

¹³ U.S. person communications may also be responsive to queries using non-U.S. person identifiers.

¹⁴ This review would not be necessary for queries seeking communications of U.S. persons who are already approved as targets for collection under Title I or Sections 703/704 of FISA and identifiers that have been approved by the FISA court under the "reasonable articulable suspicion" standard for telephony metadata under Section 215. It would also not be necessary if the query produces no results or the analyst purges all results from the given query as not containing foreign intelligence.

¹⁵ Subsequent queries using a FISA court-approved U.S. person identifier would not require court approval.

The statement also responds to the separate statement by Members Brand and Cook.

B. Separate Statement by Board Members Rachel Brand and Elisebeth Collins Cook

Board Members Rachel Brand and Elisebeth Collins Cook wrote separately to emphasize the Board's unanimous bottom-line conclusion that the core Section 702 program is clearly authorized by Congress, reasonable under the Fourth Amendment, and an extremely valuable and effective intelligence tool. They further wrote to explain their proposal for FBI queries of Section 702 data, which would not place limitations on the FBI's ability to include its FISA data within the databases *queried* in non-foreign intelligence criminal matters. They explain their view that querying information already in the FBI's possession is a relatively non-intrusive investigative tool, and the discovery of potential links between ongoing criminal and foreign intelligence investigations is potentially critical to national security. Instead, they would require an analyst who has not had FISA training to seek supervisory approval before *viewing* responsive 702 information, to ensure that the information continues to be treated consistent with applicable statutory and court-imposed restrictions. They also would require higher-level Justice Department approval before Section 702 information could be used in the investigation or prosecution of a non-foreign intelligence crime.

The statement also responds to the separate statement by Chairman Medine and Member Wald.

Part 3:

DESCRIPTION AND HISTORY

I. Genesis of the Section 702 Program

As it exists today, the Section 702 program can trace its lineage to two prior intelligence collection programs, both of which were born of counterterrorism efforts following the attacks of September 11, 2001. The first, and more well-known, of these two efforts was a program to acquire the contents of certain international communications, later termed the Terrorist Surveillance Program (“TSP”). In October 2001, President George W. Bush issued a highly classified presidential authorization directing the NSA to collect certain foreign intelligence by electronic surveillance in order to prevent acts of terrorism within the United States, based upon a finding that an extraordinary emergency existed because of the September 11 attacks. Under this authorization, electronic surveillance was permitted within the United States for counterterrorism purposes without judicial warrants or court orders for a limited number of days.¹⁶ President Bush authorized the NSA to (1) collect the contents of certain international communications, a program that was later referred to as the TSP, and (2) collect in bulk non-content information, or “metadata,” about telephone and Internet communications.¹⁷ The acquisition of telephone metadata was the forerunner to the Section 215 calling records program discussed in a prior report by the Board.

The President renewed the authorization for the NSA’s activities in early November 2001. Thereafter, the authorization was renewed continuously, with some modifications and constrictions to the scope of the authorized collection, approximately every thirty to sixty days until 2007. Each presidential authorization included the finding that an extraordinary emergency continued to exist justifying ongoing warrantless surveillance. Key members of Congress and the presiding judge of the Foreign Intelligence Surveillance Court (“FISC” or “FISA court”) were briefed on the existence of the program. The collection of communications content and bulk metadata under these presidential authorizations became known as the President’s Surveillance Program. According to a 2009 report by the inspectors general of several defense and intelligence agencies, over time, “the program

¹⁶ See DNI Announces the Declassification of the Existence of Collection Activities Authorized by President George W. Bush Shortly After the Attacks of September 11, 2001 (Dec. 21, 2013) (“Dec. 21 DNI Announcement”), available at <http://icontherecord.tumblr.com/post/70683717031/dni-announces-the-declassification-of-the>.

¹⁷ See Dec. 21 DNI Announcement, *supra*.

became less a temporary response to the September 11 terrorist attacks and more a permanent surveillance tool.”¹⁸

In December 2005, the *New York Times* published articles revealing the TSP, i.e., the portion of the President’s Surveillance Program that involved intercepting the contents of international communications. In response to these revelations, President Bush confirmed the existence of the TSP,¹⁹ and the Department of Justice issued a “white paper” outlining the legal argument that the President could authorize these interceptions without obtaining a warrant or court order.²⁰ Notwithstanding this legal argument, the government decided to seek authorization under the Foreign Intelligence Surveillance Act (“FISA”) to conduct the content collection that had been occurring under the TSP.²¹ In January 2007, the FISC issued orders authorizing the government to conduct certain electronic surveillance of telephone and Internet communications carried over listed communication facilities where, among other things, the *government* made a probable cause determination regarding one of the communicants, and the email addresses and telephone numbers to be tasked were reasonably believed to be used by persons located outside the United States.²²

The FISC’s order, referred to as the “Foreign Telephone and Email Order,” in effect replaced the President’s authorization of the TSP, and the President made no further reauthorizations of the TSP.²³ When the government sought to renew the January 2007 Foreign Telephone and Email Order, however, a different judge on the FISC approved the program, but on a different legal theory that required changes in the collection program.²⁴ Specifically, in May 2007 the FISC approved a modified version of the Foreign Telephone and Email Order in which the *court*, as opposed to the *government*, made probable cause determinations regarding the particular foreign telephone numbers and email addresses that were to be used to conduct surveillance under this program.²⁵ Although the modified

¹⁸ See UNCLASSIFIED REPORT ON THE PRESIDENT’S SURVEILLANCE PROGRAM, PREPARED BY THE OFFICE OF INSPECTORS GENERAL OF THE DEPARTMENT OF DEFENSE, DEPARTMENT OF JUSTICE, CENTRAL INTELLIGENCE AGENCY, NATIONAL SECURITY AGENCY, AND THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, at 31 (2009).

¹⁹ See, e.g., President’s Radio Address (Dec. 17, 2005), available at <http://georgewbush-whitehouse.archives.gov/news/releases/2005/12/20051217.html>.

²⁰ Legal Authorities Supporting the Activities of the National Security Agency Described by the President (January 19, 2006), available at <http://www.justice.gov/olc/opiniondocs/nsa-white-paper.pdf>.

²¹ See Dec. 21 DNI Announcement, *supra*.

²² Declassified Certification of Attorney General Michael B. Mukasey, at ¶ 37, *In re National Security Agency Telecommunications Records Litigation*, MDL Dkt. No. 06-1791-VRW (N.D. Cal. Sept. 19, 2008) (“2008 Mukasey Decl.”), available at <http://www.dni.gov/files/documents/0505/AG%20Mukasey%202008%20Declassified%20Declaration.pdf>.

²³ 2008 Mukasey Decl., *supra*, at ¶ 37.

²⁴ 2008 Mukasey Decl., *supra*, at ¶ 38 & n.20.

²⁵ 2008 Mukasey Decl., *supra*, at ¶ 38.

Foreign Telephone and Email Order permitted the government to add newly discovered telephone numbers and email addresses without an individual court order in advance,²⁶ the government assessed that the restrictions of the order, particularly after the May 2007 modifications, was creating an “intelligence gap.”²⁷

Separate from, but contemporaneous with, the TSP and the Foreign Telephone and Email Orders, a second collection effort was being undertaken. Specifically, the government used the then-existing FISA statute to obtain individual court orders to compel private companies to assist the government in acquiring the communications of individuals located overseas who were suspected of engaging in terrorism and who used United States–based communication service providers.²⁸ The government stated that it and the Foreign Intelligence Surveillance Court (FISC) expended “considerable resources” to obtain court orders based upon a probable cause showing that these overseas individuals met the legal standard for electronic surveillance under FISA,²⁹ i.e., that the targets were agents of a foreign power (such as an international terrorist group) and that they used the specific communication facilities (such as email addresses) regarding which the government was seeking to conduct electronic surveillance.³⁰ The persons targeted by these efforts were located outside the United States, and the communications being sought were frequently with others who were also located outside the United States.³¹

Drafting applications that demonstrated satisfaction of this probable cause standard, the government has asserted, slowed and in some cases prevented the acquisition of foreign intelligence information.³² The government has not disclosed the scale of this second effort to target foreign individuals using traditional FISA electronic surveillance authorities, but in the years following the passage of the Protect America Act of 2007 and the FISA Amendments Act of 2008, which eliminated the requirement for the

²⁶ 2008 Mukasey Decl., *supra*, at ¶ 38.

²⁷ See S. Rep. No. 110-209, at 5 (2007) (stating that “the DNI informed Congress that the decision . . . had led to degraded capabilities”); Eric Lichtblau, James Risen, and Mark Mazzetti, *Reported Drop in Surveillance Spurred a Law*, NEW YORK TIMES (Aug. 11, 2007) (reporting on Administration interactions with Congress that led to the enactment of the Protect America Act, including reported existence of an “intelligence gap”).

²⁸ Statement of Kenneth L. Wainstein, Assistant Attorney General, *Senate Select Committee on Intelligence Hearing On Modernization of the Foreign Intelligence Surveillance Act*, at 6-7 (May 1, 2007) (“May 2007 Wainstein Statement”), available at <http://www.intelligence.senate.gov/070501/wainstein.pdf>.

²⁹ May 2007 Wainstein Statement, *supra*, at 6-7.

³⁰ 50 U.S.C. § 1805(a)(2).

³¹ May 2007 Wainstein Statement, *supra*, at 7.

³² See, e.g., May 2007 Wainstein Statement, *supra*, at 7.

government to seek such individual orders, the total number of FISA electronic surveillance applications approved by the FISC dropped by over forty percent.³³

In light of the perceived growing inefficiencies of obtaining FISC approval to target persons located outside the United States, in the spring of 2007 the Bush Administration proposed modifications to FISA.³⁴ Reports by the Director of National Intelligence to Congress that implementation of the FISC's May 2007 modifications to the Foreign Telephone and Email Order had resulted in "degraded" acquisition of communications, combined with reports of a "heightened terrorist threat environment," accelerated Congress' consideration of these proposals.³⁵ In August 2007, Congress enacted and the President signed the Protect America Act of 2007,³⁶ a legislative forerunner to what is now Section 702 of FISA. The Protect America Act was a temporary measure that was set to expire 180 days after its enactment.³⁷

The government transitioned the collection of communications that had been occurring under the Foreign Telephone and Email Orders (previously the TSP) and some portion of the collection targeting persons located outside the United States that had been occurring under individual FISA orders to directives issued under the Protect America Act.³⁸ The Protect America Act expired in February 2008,³⁹ but existing Protect America Act certifications remained in effect until they expired.⁴⁰

Shortly after passage of the Protect America Act, efforts began to replace it with a more permanent statute.⁴¹ After substantial debate, in July 2008 Congress enacted and President Bush signed into law the FISA Amendments Act of 2008.⁴² The FISA Amendments

³³ Compare 2007 ANNUAL FISA REPORT (2,371 Title I FISA applications in 2007), available at <http://www.fas.org/irp/agency/doj/fisa/2007rept.pdf> with 2009 ANNUAL FISA REPORT (1,329 Title I FISA applications in 2009), available at <http://www.fas.org/irp/agency/doj/fisa/2009rept.pdf>.

³⁴ See S. Rep. No. 110-209, at 2, 5 (noting Administration's submission of proposed modifications in April 2007); see generally May 2007 Wainstein Statement, *supra*; Statement of J. Michael McConnell, Director of National Intelligence, Before the Senate Select Committee on Intelligence (May 1, 2007), available at <http://www.intelligence.senate.gov/070501/mcconnell.pdf>.

³⁵ See S. Rep. No. 110-209, at 5.

³⁶ Pub. L. No. 110-55; 121 Stat. 552 (2007) ("Protect America Act").

³⁷ Protect America Act § 6(c).

³⁸ 2008 Mukasey Decl., *supra*, at ¶ 13 & n.22.

³⁹ See Protect America Act—Extension, Pub. L. No. 110-182, 122 Stat. 605 (2008) (extending Protect America Act for two weeks).

⁴⁰ Protect America Act § 6.

⁴¹ See, e.g., Press Release, The White House, President Bush Discusses the Protect America Act of 2007 (Sept. 19, 2007), available at <http://georgewbush-whitehouse.archives.gov/news/releases/2007/09/20070919.html>; S. Rep. No. 110-209, at 5.

⁴² Pub. L. No. 110-261, 122 Stat. 2436 (2008).

Act replaced the expired Protect America Act provisions with the new Section 702 of FISA. The authorities and limitations of Section 702 are discussed in detail in this Report. In addition to Section 702, the FISA Amendments Act of 2008 also enacted Sections 703 and 704 of FISA, which required judicial approval for targeting U.S. persons located abroad in order to acquire foreign intelligence information.⁴³

After passage of the FISA Amendments Act, the government transitioned the collection activities that had been conducted under the Protect America Act to Section 702.⁴⁴ Section 702, as well as the other provisions of FISA enacted by the FISA Amendments Act, were renewed in December 2012, and are currently set to expire in December 2017.⁴⁵

II. Statutory Structure: What Does Section 702 Authorize?

The Foreign Intelligence Surveillance Act is a complex law, and Congress' authorization of surveillance under Section 702 of FISA is no exception. In one sentence, the statutory scope of Section 702 can be defined as follows: Section 702 of FISA permits the Attorney General and the Director of National Intelligence to jointly authorize the (1) targeting of persons who are not United States persons, (2) who are reasonably believed to be located outside the United States, (3) with the compelled assistance of an electronic communication service provider, (4) in order to acquire foreign intelligence information.⁴⁶ Each of these terms is, to various degrees, further defined and limited by other aspects of FISA. Congress also imposed a series of limitations on any surveillance conducted under Section 702. The statute further specifies how the Attorney General and Director of National Intelligence may authorize such surveillance, as well as the role of the FISC in reviewing these authorizations. This section describes this complex statutory framework.

A. Statutory Definitions and Limitations

Our description of Section 702's statutory authorization begins by breaking down the four-part sentence above.

First, Section 702 authorizes the *targeting of persons*.⁴⁷ FISA does not define what constitutes "targeting," but it does define what constitutes a "person." Persons are not only

⁴³ 50 U.S.C. §§ 1881b, 1881c.

⁴⁴ 2008 Mukasey Decl., *supra*, at ¶ 40 & n.22.

⁴⁵ FISA Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238, 126 Stat. 1631 (2012).

⁴⁶ 50 U.S.C. § 1881a(a), (b)(3), (g)(2)(A)(vi).

⁴⁷ 50 U.S.C. § 1881a(a).

individuals, but also groups, entities, associations, corporations, or foreign powers.⁴⁸ The definition of “person” is therefore broad, but not limitless: a foreign government or international terrorist group could qualify as a “person,” but an entire foreign country cannot be a “person” targeted under Section 702.⁴⁹ In addition, the persons whom may be targeted under Section 702 may not intentionally include United States persons.⁵⁰ “United States persons” or “U.S. persons” are United States citizens, United States permanent residents (green card holders), groups substantially composed of United States citizens or permanent residents, and virtually all United States corporations.⁵¹ As is discussed in detail below, the NSA targets persons by tasking “selectors,” such as email addresses and telephone numbers. The NSA must make 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 terrorist group.

Second, under Section 702 the non-U.S. person target *must also be “reasonably believed to be located outside the United States.”* A “reasonable belief” is not defined in FISA, but Section 702 does require that targeting procedures (described in further detail below) be adopted to ensure that Section 702 acquisition is limited to targets reasonably believed to be located outside the United States.⁵² Electronic surveillance targeting persons believed to be located in the United States is not permitted by Section 702, whether the persons in question are U.S. persons or not.⁵³

Third, under Section 702 this targeting of non-U.S. persons reasonably believed to be located outside the United States *occurs with the compelled assistance of an “electronic communication service provider.”*⁵⁴ FISA defines electronic communication service providers to include a variety of telephone, Internet service, and other communications providers.⁵⁵ As further described below, electronic communication service providers are

⁴⁸ 50 U.S.C. §§ 1801(m), 1881(a). The term “foreign power” is a defined term in FISA; it includes international terrorist groups, foreign governments, and entities not substantially composed of United States persons that are engaged in the proliferation of weapons of mass destruction.

⁴⁹ See Privacy and Civil Liberties Oversight Board, Transcript of Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, at 71 (Mar. 19, 2014) (“PCLOB March 2014 Hearing Transcript”) (statement of Rajesh De, General Counsel, NSA, in response to questions by James Dempsey, Board Member, PCLOB), *available at* http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/19-March-2014_Public_Hearing_Transcript.pdf.

⁵⁰ 50 U.S.C. § 1881a(b)(3).

⁵¹ 50 U.S.C. § 1801(i).

⁵² 50 U.S.C. § 1881a(d)(1)(A).

⁵³ 50 U.S.C. §§ 1881(b)(1).

⁵⁴ 50 U.S.C. § 1881a(g)(2)(A)(vi).

⁵⁵ 50 U.S.C. § 1881(b)(4).

compelled to provide this assistance in conducting Section 702 acquisition through directives issued by the Attorney General and the Director of National Intelligence. Given the nature of the Internet, communications generated and delivered through communication services offered directly to individuals by one entity may be acquired as they cross the network of another provider without the knowledge of the consumer-facing provider. This concept is further described in the discussion below regarding upstream collection.

Fourth, and finally, this targeting of non-U.S. persons reasonably believed to be located outside the United States *must be conducted "to acquire foreign intelligence information."*⁵⁶ Non-U.S. persons may be targeted under Section 702 only if the government has reason to believe that those persons possess, are expected to receive, or are likely to communicate foreign intelligence information.⁵⁷ Foreign intelligence information concerning non-U.S. persons is defined in FISA as information that relates to the ability of the United States to protect against an actual or potential attack by a foreign power; sabotage, international terrorism, or the proliferation of weapons of mass destruction by a foreign power; or clandestine intelligence activities by a foreign power.⁵⁸ Foreign

⁵⁶ There is some conflicting language in Section 702 on the precise standard on this point. Section 1881a(a) states that a Section 702 authorization must be "...to acquire foreign intelligence information." This authority, however, must be governed by a certification, and the certification need only state that "a significant purpose of the acquisition is to obtain foreign intelligence information." 50 U.S.C. § 1881a(g)(2)(A)(v). *See also* SEMI-ANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUES PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, AUGUST 2013, at A-2 ("AUGUST 2013 SEMI-ANNUAL ASSESSMENT") (noting that the Section 702 Attorney General Guidelines implement the statutory requirement that a "significant purpose of [Section 702] acquisition is to obtain foreign intelligence information," 50 U.S.C. § 1881a(g)(2)(A)(v), by requiring that Section 702 targeting occur only with respect to persons assessed to possess foreign intelligence information or who are reasonably likely to receive or communicate foreign intelligence information), *available at* <http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf>; *see also* NSA DIRECTOR OF CIVIL LIBERTIES AND PRIVACY OFFICE REPORT: NSA'S IMPLEMENTATION OF FOREIGN INTELLIGENCE SURVEILLANCE ACT SECTION 702, at 5 (April 16, 2014) ("NSA DCLPO REPORT"), *available at* <http://www.dni.gov/files/documents/0421/702%20Unclassified%20Document.pdf>.

⁵⁷ NSA DCLPO REPORT, *supra*, at 3.

⁵⁸ 50 U.S.C. § 1801(e)(1). For information concerning a U.S. person, the information must be "necessary" for this purpose. Specifically, this provision states foreign intelligence information is defined as:

[I]nformation 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 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.

intelligence information concerning non-U.S. persons is also defined as information that relates to the national defense or security of the United States or the conduct of the foreign affairs of the United States, but only insofar as that information concerns a foreign power (such as international terrorist groups or foreign governments) or foreign territory.⁵⁹ The term “foreign territory” is undefined by the statute. As noted below, in authorizing Section 702 acquisition, the Attorney General and Director of National Intelligence specify the categories of foreign intelligence information that the United States government is seeking to acquire.

In addition to defining the scope of the Section 702 authorization, Congress specified limitations on the government’s authority to engage in Section 702 targeting. As previously mentioned, U.S. persons may not be intentionally targeted. In addition, the government is prohibited under the law from intentionally targeting “any person known at the time of acquisition to be located in the United States.”⁶⁰ These two rules taken together — that the target must be both a non-U.S. person and someone reasonably believed to be located abroad — are often referred to as the “foreignness” requirement.

The government is also prohibited from engaging in what is generally referred to as “reverse targeting,” which would occur if the government were to intentionally target persons reasonably believed to be located outside the United States “if the purpose of the acquisition is to target a particular, known person reasonably believed to be in the United States.”⁶¹ In addition to this explicit prohibition against reverse targeting persons located in the United States, the government reads the statutory prohibition against targeting U.S. persons to also prohibit the reverse targeting of U.S. persons.⁶² In other words, the ban on reverse targeting prohibits the government from targeting a non-U.S. person outside the United States when the real interest is to collect the communications of a person in the United States or of any U.S. person, regardless of location.

Under Section 702, the government also “may not intentionally acquire communications as to which the sender and all intended recipients are known at the time

⁵⁹ 50 U.S.C. § 1801(e)(2). Specifically, this provision states foreign intelligence information is also defined as:

[I]nformation 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.

⁶⁰ 50 U.S.C. § 1881a(b)(1).

⁶¹ 50 U.S.C. § 1881a(b)(2).

⁶² See PCLOB March 2014 Hearing Transcript, *supra*, at 89-92.

of the acquisition to be located in the United States.”⁶³ Finally, Section 702 contains a limitation (and a reminder) that any acquisition must always be conducted consistent with the requirements of the Fourth Amendment to the Constitution.⁶⁴

B. Section 702 Certifications

The Attorney General and the Director of National Intelligence authorize Section 702 targeting in a manner substantially different than traditional electronic surveillance under FISA. To authorize traditional FISA electronic surveillance, an application approved by the Attorney General must be made to the FISC.⁶⁵ This individualized application must include, among other things, the identity (if known) of the specific target of the electronic surveillance; facts justifying a probable cause finding that this target is a foreign power or agent of a foreign power and uses (or is about to use) the communication facilities or places at which electronic surveillance is being directed;⁶⁶ minimization procedures governing the acquisition, retention, and dissemination of non-publicly available U.S. person information acquired through the electronic surveillance; and a certification regarding the foreign intelligence information sought.⁶⁷ If the FISC judge who reviews the government’s application determines that it meets the required elements — including that there is probable cause that the specified target is a foreign power or agent of a foreign power and that the minimization procedures meet the statutory requirements — the judge will issue an order authorizing the requested electronic surveillance.⁶⁸

Section 702 differs from this traditional FISA electronic surveillance framework both in the standards applied and in the lack of individualized determinations by the FISC. Under the statute, the Attorney General and Director of National Intelligence make annual certifications authorizing the targeting of non-U.S. persons reasonably believed to be located outside the United States to acquire foreign intelligence information, without specifying to the FISC the particular non-U.S. persons who will be targeted.⁶⁹ Instead of identifying particular individuals to be targeted under Section 702, the certifications identify categories of foreign intelligence information regarding which the Attorney

⁶³ 50 U.S.C. § 1881a(b)(4).

⁶⁴ 50 U.S.C. § 1881a(b)(5).

⁶⁵ 50 U.S.C. § 1804(a). FISA also grants additional authority to conduct emergency electronic surveillance without first making an application to the FISC. 50 U.S.C. § 1805(e).

⁶⁶ *But see* 50 U.S.C. § 1805(c)(3) (permitting electronic surveillance orders “in circumstances where the nature and location of each of the facilities or places at which surveillance will be directed is unknown”)

⁶⁷ 50 U.S.C. §§ 1804(a), 1805(a).

⁶⁸ 50 U.S.C. § 1805(a), (c), (d).

⁶⁹ 50 U.S.C. § 1881a(a); NSA DCLPO REPORT, *supra*, at 2 (noting that Section 702 certifications do not require “individualized determination” by the FISC).

General and Director of National Intelligence authorize acquisition through the targeting of non-U.S. persons reasonably believed to be located abroad.⁷⁰ There also is no requirement that the government demonstrate probable cause to believe that a Section 702 target is a foreign power or agent of a foreign power, as is required under traditional FISA. Rather, the categories of information being sought must meet the definition of foreign intelligence information described above. The government has not declassified the full scope of the certifications that have been authorized, but officials have stated that these certifications have authorized the acquisition of information concerning international terrorism and other topics, such as the acquisition of weapons of mass destruction.⁷¹

While individual targets are not specified, Section 702 certifications must instead contain “targeting procedures” approved by the Attorney General that must 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 prevents the “intentional acquisition” of wholly domestic communications.⁷² The targeting procedures specify the manner in which the Intelligence Community must determine whether a person is a non-U.S. person reasonably believed to be located outside the United States who possesses (or is likely to possess or receive) the types of foreign intelligence information authorized by a certification. The process by which individuals are permitted to be targeted pursuant to the targeting procedures is discussed in detail below. In addition, the Attorney General and Director of National Intelligence must also attest in the certification that the Attorney General has adopted additional guidelines to ensure compliance with both these and the other statutory limitations on the Section 702 program.⁷³ Most critically, these Attorney General Guidelines explain how the government implements the statutory prohibition against reverse targeting.

While only non-U.S. persons may be intentionally targeted, the information of or concerning U.S. persons may be acquired through Section 702 targeting in a variety of ways, such as when a U.S. person is in communication with a non-U.S. person Section 702

⁷⁰ See 50 U.S.C. § 1881a(g)(2)(A)(v) (requiring Attorney General and Director of National Intelligence to attest that a significant purpose of the acquisition authorized by the certification is to acquire foreign intelligence information); PCLOB March 2014 Hearing Transcript, *supra*, at 8-9 (statement of Robert Litt, General Counsel, ODNI) (stating that certifications “identify categories of information that may be acquired”); NSA DCLPO REPORT, *supra*, at 2 (noting the “annual topical certifications” authorized by Section 702).

⁷¹ PCLOB March 2014 Hearing Transcript at 13 (statement of Robert Litt, General Counsel, ODNI) (stating that the Section 702 program has been an important source of information “not only about terrorism, but about a wide variety of other threats to our nation”); *id.* at 59 (statement of Rajesh De, General Counsel, NSA) (stating that there are certifications on “counterterrorism” and “weapons of mass destruction”); *id.* at 68 (statement of James A. Baker, General Counsel, FBI) (“[T]his program is not limited just to counterterrorism.”).

⁷² 50 U.S.C. § 1881a(d)(1), (g)(2)(A)(i), (g)(2)(B).

⁷³ 50 U.S.C. § 1881a(f), (g)(2)(A)(iii).

target, because two non-U.S. persons are discussing a U.S. person, or because a U.S. person was mistakenly targeted. Section 702 therefore requires that certifications also include “minimization procedures” that control the acquisition, retention, and dissemination of any non-publicly available U.S. person information acquired through the Section 702 program.⁷⁴ As discussed below, the minimization procedures include different procedures for handling U.S. person information depending on the circumstances of how it was acquired. Along with the targeting procedures, the minimization procedures contain the government’s core privacy and civil liberties protections and are more fully discussed throughout this Report.

C. FISC Review

The government’s Section 702 certifications, targeting procedures, and minimization procedures (but not the Attorney General Guidelines) are all subject to review by the FISC.⁷⁵ In addition to the required procedures and guidelines, the Section 702 certifications are accompanied by affidavits of national security officials⁷⁶ that further describe to the FISC the government’s basis for assessing that the proposed Section 702 acquisition will be consistent with the applicable statutory authorization and limits.⁷⁷ Through court filings or the testimony of witnesses at hearings before the FISC, the government also submits additional information explaining how the targeting and minimization procedures will be applied and describing the operation of the program in a way that defines its scope.⁷⁸

The FISC’s review of the Section 702 certifications has been called “limited” by scholars,⁷⁹ privacy advocates,⁸⁰ and in one instance, shortly after the FISA Amendments Act

⁷⁴ 50 U.S.C. § 1881a(e)(1), (g)(2)(A)(ii), (g)(2)(B).

⁷⁵ 50 U.S.C. § 1881a(d)(2), (e)(2), (i). The Attorney General Guidelines must, however, be submitted to the FISA court. 50 U.S.C. § 1881a(f)(2)(C). Section 702 does have a provision permitting the Attorney General and the Director of National Intelligence to authorize acquisition prior to judicial review of a certification under certain exigent circumstances. 50 U.S.C. § 1881a(c)(2). To date, the Attorney General and the Director of National Intelligence have never exercised this authority.

⁷⁶ 50 U.S.C. § 1881a(g)(2)(C); *see, e.g.*, Memorandum Opinion at 3, [*Caption Redacted*], [Docket No. Redacted], 2011 WL 10945618, at *1 (FISA Ct. Oct. 3, 2011) (“Bates October 2011 Opinion”) (noting submitted affidavits by the Director or Acting Director of NSA and the Director of FBI), *available at* <http://icontherecord.tumblr.com/post/58944252298/dni-declassifies-intelligence-community-documents>.

⁷⁷ *See* AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-1 to A-2.

⁷⁸ *See, e.g.*, Bates October 2011 Opinion, *supra*, at 5-9, 2011 WL 10945618, at *2-4 (describing 2011 government filings with, and testimony before, the FISA court); *id.* at 15-16, 2011 WL 10945618, at *5 (describing representations made to the FISA court in prior Section 702 certifications).

⁷⁹ *See, e.g.*, Laura K. Donohue, Section 702 and the Collection of International Telephone and Internet Content, at 15, 18, 30-34, *available at* <http://justsecurity.org/wp-content/uploads/2014/05/donahue.702.pdf>.

was passed, by the FISC itself.⁸¹ In certain respects, this characterization is accurate. Unlike traditional FISA applications, the FISC does not review the targeting of particular individuals. Specifically, although the Section 702 certifications identify the foreign intelligence subject matters regarding which information is to be acquired, the FISC does not see or approve the specific persons targeted or the specific communication facilities that are actually tasked for acquisition. As such the government does not present evidence to the FISC, nor does the FISC determine — under probable cause or any other standard — that the particular individuals being targeted are non-U.S. persons reasonably believed to be located outside the United States who are being properly targeted to acquire foreign intelligence information.⁸² Instead of requiring judicial review of these elements, Section 702 calls upon the FISA court only to decide whether the targeting procedures are reasonably designed to ensure compliance with certain limitations and that the minimization procedures satisfy certain criteria (described below). The FISC is not required to independently determine that a significant purpose of the proposed acquisition is to obtain foreign intelligence information,⁸³ although the foreign intelligence purpose of the collection does play a role in the court's Fourth Amendment analysis.⁸⁴

In other respects, however, the FISC's role in the Section 702 program is more extensive. The FISC reviews both the targeting procedures and the minimization procedures, the core set of documents that implement Section 702's statutory requirements and limitations.⁸⁵ With respect to the targeting procedures, the FISC must

⁸⁰ See, e.g., Submission of Jameel Jaffer, Deputy Legal Director, American Civil Liberties Union Foundation, Privacy and Civil Liberties Oversight Board Public Hearing on Section 702 of the FISA Amendments Act, at 9 (Mar. 19, 2014), available at http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/Testimony_Jaffer.pdf.

⁸¹ Memorandum Opinion, *In re Proceedings Required by § 702(i) of the FISA Amendments Act of 2008*, Docket Misc. No. 08-01, 2008 WL 9487946, at *5 (FISA Ct. Aug. 27, 2008).

⁸² See The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, at 2 (2012) (describing differences between targeting individuals under traditional FISA electronic surveillance provisions and targeting pursuant to Section 702). This document accompanied a 2012 letter sent by the Department of Justice and the Office of the Director of National Intelligence to the Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence urging the reauthorization of Section 702. See Letter from Kathleen Turner, Director of Legislative Affairs, ODNI, and Ronald Weich, Assistant Attorney General, Office of Legislative Affairs, DOJ to the Honorable Dianne Feinstein, Chairman, Senate Committee on Intelligence, et. al. (May 4, 2012), available at http://www.dni.gov/files/documents/Ltr%20to%20HPSCI%20Chairman%20Rogers%20and%20Ranking%20Member%20Ruppersberger_Scan.pdf.

⁸³ 50 U.S.C. § 1881a(i)(2).

⁸⁴ Additionally, if the FISC determines that a Section 702 certification and related documents are insufficient on Constitutional or statutory grounds, the FISC cannot itself modify the certification and related documents governing the Section 702 program, but instead must issue an order to the government to either correct any deficiencies identified by the FISC within 30 days or to cease (or not begin) implementation of the certification. 50 U.S.C. § 1881a(i)(3)(B).

⁸⁵ 50 U.S.C. § 1881a(d)(2), (e)(2), (i)(1)(A).

determine that they “are reasonably designed” to “ensure” that targeting is “limited to targeting persons reasonably believed to be located outside the United States.”⁸⁶ The FISC also must determine that the targeting procedures are reasonably designed to prevent the intentional acquisition of wholly domestic communications.⁸⁷ In addition, the FISC must also review the proposed minimization procedures under the same standard of review that is required in traditional FISA electronic surveillance and physical search applications.⁸⁸ The FISC must find that such minimization procedures are “specific procedures” that are “reasonably designed” to control the acquisition, retention, and dissemination of non-publicly available U.S. person information.⁸⁹ Each time the FISC reviews a Section 702 certification, the FISC must also determine whether the proposed Section 702 acquisition as provided for, and restricted by, the targeting and minimization procedures complies with the Fourth Amendment.⁹⁰ After conducting its analysis, the FISC must issue a written opinion explaining the reasons why the court has held that the proposed targeting and minimization procedures do, or do not, comply with statutory and Fourth Amendment requirements.⁹¹

The FISC has held that it cannot make determinations in a vacuum regarding whether targeting and minimization procedures are “reasonably designed” to meet the statutory requirements and comply with the Fourth Amendment. To the contrary, the FISC “has repeatedly noted that the government’s targeting and minimization procedures must be considered in light of the communications actually acquired,” and that “[s]ubstantial implementation problems can, notwithstanding the government’s intent, speak to whether the applicable targeting procedures are ‘reasonably designed’ to acquire only the communications of non-U.S. persons outside the United States.”⁹² Therefore, although the FISC reviews the targeting procedures, minimization procedures, and related affidavits that

⁸⁶ 50 U.S.C. § 1881a(i)(2)(B)(i).

⁸⁷ 50 U.S.C. § 1881a(i)(2)(B)(ii).

⁸⁸ Compare 50 U.S.C. § 1881a(i)(2)(C) (requirement to evaluate Section 702 minimization procedures) with 50 U.S.C. § 1805(a)(3) (requirement to evaluate FISA electronic surveillance minimization procedures) and 50 U.S.C. § 1824(a)(3) (requirement to evaluate FISA physical search minimization procedures).

⁸⁹ 50 U.S.C. § 1801(h).

⁹⁰ 50 U.S.C. § 1881a(i)(3)(A), (i)(3)(B).

⁹¹ 50 U.S.C. § 1881a(i)(3)(C). While FISC judges may write opinions explaining their orders with regard to other aspects of FISA, the statutory requirement for an opinion explaining the rationale of all orders approving Section 702 certifications is unique within FISA. Though not required by FISA, FISC Rule of Procedure 18(b)(1) also requires FISC judges to provide a written statement of reasons for any denials of the government’s other FISA applications. See United States Foreign Intelligence Surveillance Court Rules of Procedure (“FISC Rule of Procedure”), Rule 18(b)(1), available at <http://www.uscourts.gov/uscourts/rules/FISC2010.pdf>.

⁹² Bates October 2011 Opinion, *supra*, at 28, 2011 WL 10945618, at *9 (quoting FISC opinion with redacted docket number).

are submitted with a Section 702 certification, the court's review is not limited to the four corners of those documents. The FISC also takes into consideration additional filings by the government to supplement or clarify the record, responses to FISC orders to supplement the record,⁹³ and the sworn testimony of witnesses at hearings.⁹⁴

Commitments regarding how the targeting and minimization procedures will be implemented that are made to the FISC in these representations have been found to be binding on the government. For example, during the consideration of the first Section 702 certification in 2008, the government stated that the targeting procedures impose a requirement that analysts conduct "due diligence" in determining the U.S. person status of any Section 702 target, even though the phrase "due diligence" is not explicitly found in the text of the NSA targeting procedures. The FISC incorporated the government's representation regarding due diligence into its opinion, and the government has subsequently reported to Congress and the FISC — as incidents of noncompliance — instances in which the Intelligence Community conducted insufficient due diligence that resulted in the targeting of a U.S. person.⁹⁵

In evaluating the Section 702 certifications, the court also considers additional filings required by the FISC's Rules of Procedure. One such rule requires the government to notify the FISA court whenever the government discovers a material misstatement or omissions in a prior filing with the court.⁹⁶ Another rule mandates that the government report to the FISA court incidents of noncompliance with targeting or minimization procedures previously approved by the court.⁹⁷ In a still-classified 2009 opinion, the FISC held that the judicial review requirements regarding the targeting and minimization procedures required that the FISC be fully informed of every incident of noncompliance

⁹³ See FISC Rule of Procedure 5(c) (stating that the FISC Judges have the authority to order any party to a proceeding to supplement the record by "furnish[ing] any information that the Judge deems necessary").

⁹⁴ FISC Rule of Procedure 17.

⁹⁵ See AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 29 (describing incidents and stating "In each of these incidents, all Section 702-acquired data was purged. Together, these [redacted] instances represent isolated instances of insufficient due diligence that do not reflect the [redacted] of taskings that occur during the reporting period.").

⁹⁶ See FISC Rule of Procedure 13(a).

⁹⁷ See FISC Rule of Procedure 13(b); SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUES PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, MAY 2010, at 22 ("MAY 2010 SEMIANNUAL ASSESSMENT") (discussing requirements under Rule 10(c), the predecessor to Rule 13(b) in the prior set of FISC Rules of Procedure), *available at* <http://www.dni.gov/files/documents/FAA/SAR%20May%202010%20Final%20Release%20with%20Exemptions.pdf>. The government also provides the FISC the Semiannual Section 702 Joint Assessment, portions of the Section 707 Semiannual report, and a separate quarterly report to the FISC, all of which describe scope, nature, and actions taken in response to compliance incidents. See *The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act*, *supra*, at 5; 50 U.S.C. § 1881a(l)(1).

with those procedures. In the 2009 opinion, the court analyzed whether several errors in applying the targeting and minimization procedures that had been reported to the court undermined either the court's statutory or constitutional analysis. (The court concluded that they did not.)

In addition to identifying errors that could impact the sufficiency of the targeting and minimization procedures, these compliance notices play an additional role in informing the FISC regarding how the government is in fact applying the targeting and minimization procedures. Specifically, the compliance notices must state both the type of noncompliance that has occurred and the facts and circumstances relevant to the incident.⁹⁸ In doing so, representations to the FISA court have in essence created a series of precedents regarding how the government is interpreting various provisions of its targeting and minimization procedures, which informs the court's conclusions regarding whether those procedures — as actually applied by the Intelligence Community to particular, real-life factual scenarios — comply with Section 702's statutory requirements and the Fourth Amendment. For example, while the 2008 FISC opinion incorporated the government's commitment to apply due diligence in determining the U.S. person status of potential targets, notices of non-compliance filed by the government reflect that the government interprets the targeting procedures to also require due diligence in determining the *location* of potential targets. Similarly, the government has filed letters clarifying aspects of its "post-tasking" process, which are discussed further below, and it has reported — as compliance incidents — instances when its performance of the post-tasking process has not complied with those representations. The government's interpretations of the targeting and minimization procedures reflected in these compliance filings, however, are not necessarily formally endorsed or incorporated into the FISC's subsequent opinions. In the Board's opinion Intelligence Community personnel applying these procedures months or years later may not be aware of the interpretive gloss arising from prior interactions between the government and the FISC on these procedures.

Former FISC Presiding Judge John Bates' October 3, 2011 opinion provides both an example of the scope of the FISA court's review of Section 702 certifications in practice and an illustration of what actions the court can take if it determines that the government has not satisfied the court's expectations to be kept fully, accurately, and timely informed. In April 2011, the government filed multiple Section 702 certifications with the FISC.⁹⁹ In early May 2011, however, the government filed a letter with the court (under a FISC procedural rule regarding material misstatements or omissions) acknowledging that the scope of the NSA's "upstream" collection (described below) was more expansive than

⁹⁸ FISC Rule of Procedure 13(b).

⁹⁹ Bates October 2011 Opinion, *supra*, at 3, 2011 WL 10945618, at *1.

previously represented to the court.¹⁰⁰ As a result of the filing, the FISC expressed serious concern that the upstream collection, as described by the government, may have exceeded the scope of collection previously approved by the FISC and what could be authorized under Section 702. The FISC therefore ordered the government to respond to a number of questions regarding the upstream collection program.¹⁰¹ Throughout the summer of 2011, the government continued to supplement the record in response to the FISA court's concerns with a number of filings, including by conducting and reporting to the court the results of a statistical sample of the NSA's acquisition of upstream collection.¹⁰² The government's supplemental filings discussed both factual matters, such as how many domestic communications were being acquired as a result of the manner in which the government was conducting upstream collection, as well as the government's legal interpretations regarding how the NSA's minimization procedures should be applied to such acquisition.¹⁰³ The FISA court also met with the government and held a hearing to ask additional questions of NSA and Department of Justice personnel.¹⁰⁴

Based on this record, Judge Bates ultimately held that in light of the new information, portions of the NSA minimization procedures met neither the requirements of FISA nor the Fourth Amendment and ordered the government to correct the deficient procedures or cease Section 702 upstream collection.¹⁰⁵ The government subsequently modified the NSA minimization procedures to remedy the deficiencies identified by the FISA court.¹⁰⁶ The FISC continued to have questions, however, regarding upstream collection that had been acquired prior to the implementation of these modified NSA minimization procedures.¹⁰⁷ The government took several actions with regard to this past upstream collection, and ultimately decided to purge it all.¹⁰⁸

¹⁰⁰ Bates October 2011 Opinion, *supra*, at 5, 2011 WL 10945618, at *2.

¹⁰¹ Bates October 2011 Opinion, *supra*, at 7, 2011 WL 10945618, at *2.

¹⁰² Bates October 2011 Opinion, *supra*, at 10, 2011 WL 10945618, at *3-4.

¹⁰³ Bates October 2011 Opinion, *supra*, at 33-35, 50, 54-56, 2011 WL 10945618, at *11, *17, *18-19.

¹⁰⁴ Bates October 2011 Opinion, *supra*, at 7-9, 2011 WL 10945618, at *4.

¹⁰⁵ Bates October 2011 Opinion, *supra*, at 59-63, 67-80, 2011 WL 10945618, at *20-28.

¹⁰⁶ See generally Memorandum Opinion, [Caption Redacted], [Docket No. Redacted], 2011 WL 10947772 (FISA Ct. Nov. 30, 2011) ("Bates November 2011 Opinion"), available at <http://icontherecord.tumblr.com/post/58944252298/dni-declassifies-intelligence-community-documents>.

¹⁰⁷ See Memorandum Opinion at 26-30, [Caption Redacted], [Docket No. Redacted], 2012 WL 9189263, at *1-4 (FISA Ct. Sept. 25, 2012) ("Bates September 2012 Opinion"), available at <http://www.dni.gov/files/documents/September%202012%20Bates%20Opinion%20and%20Order.pdf>.

¹⁰⁸ Bates September 2012 Opinion, *supra*, at 30-32, 2012 WL 9189263, at *3-4.

D. Directives

As noted above, Section 702 targeting may occur only with the assistance of electronic communication service providers. Once Section 702 acquisition has been authorized, the Attorney General and the Director of National Intelligence send written directives to electronic communication service providers compelling the providers' assistance in the acquisition.¹⁰⁹ Providers that receive a Section 702 directive may challenge the legality of the directive in the FISC.¹¹⁰ The government may likewise file a petition with the FISC to compel a provider that does not comply with a directive to assist the government's acquisition of foreign intelligence information.¹¹¹ The FISC's decisions regarding challenges and enforcement actions regarding directives are appealable to the Foreign Intelligence Surveillance Court of Review ("FISCR"), and either the government or a provider may request that the United States Supreme Court review a decision of the FISCR.¹¹²

III. Acquisition Process: How Does Section 702 Surveillance Actually Work?

Once a Section 702 certification has been approved, non-U.S. persons reasonably believed to be located outside the United States may be targeted to acquire foreign intelligence information within the scope of that certification. The process by which non-U.S. persons are targeted is detailed in the next section. This section describes how Section 702 acquisition takes place once an individual has been targeted.

A. Targeting Persons by Tasking Selectors

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, such as the target's email address or telephone number.¹¹³ 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

¹⁰⁹ 50 U.S.C. § 1881a(h).

¹¹⁰ 50 U.S.C. § 1881a(h)(4).

¹¹¹ 50 U.S.C. § 1881a(h)(5).

¹¹² 50 U.S.C. § 1881a(h)(6). However, as noted in the Board's Section 215 report, to date, only two cases have been appealed to the FISCR. One, *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004 (FISA Ct. Rev. 2008), involved a directive under the Protect America Act, the predecessor to Section 702, but none have involved Section 702. Nor has the U.S. Supreme Court ever considered the merits of a FISA order or ruled on the merits of any challenge to FISA.

¹¹³ See AUGUST 2013 JOINT ASSESSMENT, *supra*, at A-2; NSA DCLPO REPORT, *supra*, at 4; The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3.

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”).¹¹⁴ 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.¹¹⁵

Although targeting decisions must be individualized, this does not mean that a substantial number of persons are not targeted under the Section 702 program. The government estimates that 89,138 persons were targeted under Section 702 during 2013.¹¹⁶

Once a selector has been tasked under the targeting procedures, it is sent to an electronic communications service provider to begin acquisition. There are two types of Section 702 acquisition: what has been referred to as “PRISM” collection and “upstream” collection. PRISM collection is the easier of the two acquisition methods to understand.

B. PRISM Collection

In PRISM collection, the government (specifically, the FBI on behalf of the NSA) sends selectors — such as an email address — to a United States–based electronic communications service provider (such as an Internet service provider, or “ISP”) that has been served a directive.¹¹⁷ Under the directive, the service provider is compelled to give the communications sent to or from that selector to the government (but not communications that are only “about” the selector, as described below).¹¹⁸ As of mid-2011, 91 percent of the

¹¹⁴ NSA DCLPO REPORT, *supra*, at 4; PCLOB March 2014 Hearing Transcript, *supra*, at 57 (statement of Rajesh De, General Counsel, NSA) (noting that a name cannot be tasked).

¹¹⁵ NSA DCLPO REPORT, *supra*, at 6.

¹¹⁶ OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE STATISTICAL TRANSPARENCY REPORT REGARDING USE OF NATIONAL SECURITY AUTHORITIES: ANNUAL STATISTICS FOR CALENDAR YEAR 2013, at 1 (June 26, 2014), available at http://www.dni.gov/files/tp/National_Security_Authorities_Transparency_Report_CY2013.pdf. In calculating this estimate, the government counted two known people using one tasked email address as two targets and one person known to use two tasked email addresses as one target. The number of targets is an estimate because the government may not be aware of all of the users of a particular tasked selector.

¹¹⁷ The Intelligence Community’s Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3. See also PCLOB March 2014 Hearing Transcript at 70 (statement of Rajesh De, General Counsel, NSA) (noting any recipient company “would have received legal process”).

¹¹⁸ PCLOB March 2014 Hearing Transcript at 70; see also NSA DCLPO REPORT, *supra*, at 5.

Internet communications that the NSA acquired each year were obtained through PRISM collection.¹¹⁹

The government has not declassified the specific ISPs that have been served directives to undertake PRISM collection, but an example using a fake United States company (“USA-ISP Company”) may clarify how PRISM collection works in practice: The NSA learns that John Target, a non-U.S. person located outside the United States, uses the email address “johntarget@usa-ISP.com” to communicate with associates about his efforts to engage in international terrorism. The NSA applies its targeting procedures (described below) and “tasks” johntarget@usa-ISP.com to Section 702 acquisition for the purpose of acquiring information about John Target’s involvement in international terrorism. The FBI would then contact USA-ISP Company (a company that has previously been sent a Section 702 directive) and instruct USA-ISP Company to provide to the government all communications to or from email address johntarget@usa-ISP.com. The acquisition continues until the government “detasks” johntarget@usa-ISP.com.

The NSA receives all PRISM collection acquired under Section 702. In addition, a copy of the raw data acquired via PRISM collection — and, to date, only PRISM collection — may also be sent to the CIA and/or FBI.¹²⁰ The NSA, CIA, and FBI all must apply their own minimization procedures to any PRISM-acquired data.¹²¹

Before data is entered into systems available to trained analysts or agents, government technical personnel use technical systems to help verify that data sent by the provider is limited to the data requested by the government. To again use the John Target example above, if the NSA determined that johntarget@usa-ISP.com was not actually going to be used to communicate information about international terrorism, the government would send a detasking request to USA-ISP Company to stop further Section 702 collection on this email address. After passing on the detasking request to USA-ISP Company, the government would use its technical systems to block any further Section 702 acquisition from johntarget@usa-ISP.com to ensure that Section 702 collection against this address was immediately terminated.

¹¹⁹ Bates October 2011 Opinion, *supra*, at 29-30 and n.24, 2011 WL 10945618, at *25 & n.24.

¹²⁰ 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, § 6(c) (Oct. 31, 2011) (“NSA 2011 Minimization Procedures”), *available at* <http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf>.

¹²¹ NSA 2011 Minimization Procedures, *supra*, § 6(c).

C. Upstream Collection

The NSA acquires communications from a second means, which is referred to as upstream collection. Upstream collection is different from PRISM collection because the acquisition occurs not with the compelled assistance of the United States ISPs, but instead with the compelled assistance (through a Section 702 directive) of the providers that control the telecommunications backbone over which communications transit.¹²² The collection therefore does not occur at the local telephone company or email provider with whom the targeted person interacts (which may be foreign telephone or Internet companies, which the government cannot compel to comply with a Section 702 directive), but instead occurs “upstream” in the flow of communications between communication service providers.¹²³

Unlike PRISM collection, raw upstream collection is not routed to the CIA or FBI, and therefore it resides only in NSA systems, where it is subject to the NSA’s minimization procedures.¹²⁴ CIA and FBI personnel therefore lack any access to raw data from upstream collection. Accordingly, they cannot view or query such data in CIA or FBI systems.

The upstream acquisition of telephone and Internet communications differ from each other, and these differences affect privacy and civil liberty interests in varied ways.¹²⁵ Each type of Section 702 upstream collection is discussed below. In conducting both types of upstream acquisition, NSA employs certain collection monitoring programs to identify anomalies that could indicate that technical issues in the collection platform are causing data to be overcollected.¹²⁶

¹²² The Intelligence Community’s Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3-4; *see also* PCLOB March 2014 Hearing Transcript, *supra*, at 26 (statement of Rajesh De, General Counsel, NSA) (“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.”).

¹²³ *See* PCLOB March 2014 Hearing Transcript, *supra*, at 26 (statement of Rajesh De, General Counsel, NSA) (“This type of collection upstream fills a particular gap of allowing us to collect communications that are not available under PRISM collection.”).

¹²⁴ The Intelligence Community’s Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 4.

¹²⁵ *See* PCLOB March 2014 Hearing Transcript, *supra*, at 27 (statement of Rajesh De, General Counsel, NSA).

¹²⁶ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 29.

1. Upstream Collection of Telephone Communications

Like PRISM collection, the upstream collection of telephone communications begins with the NSA's tasking of a selector.¹²⁷ The same targeting procedures that govern the tasking of an email address in PRISM collection also apply to the tasking of a telephone number in upstream collection.¹²⁸ Prior to tasking, the NSA therefore is required to assess that the specific telephone number to be tasked is used by a non-U.S. person reasonably believed to be located outside the United States from whom the NSA assesses it may acquire the types of foreign intelligence information authorized under one of the Section 702 certifications. Once the targeting procedures have been applied, the NSA sends the tasked telephone number to a United States electronic communication service provider to initiate acquisition.¹²⁹ The communications acquired, with the compelled assistance of the provider, are limited to telephone communications that are either to or from the tasked telephone number that is used by the targeted person. Upstream telephony collection therefore does not acquire communications that are merely "about" the tasked telephone number.¹³⁰

2. Upstream Collection of Internet "Transactions"

The process of tasking selectors to acquire Internet transactions is similar to tasking selectors to PRISM and upstream telephony acquisition, but the actual acquisition is substantially different. Like PRISM and upstream telephony acquisition, the NSA may only target non-U.S. persons by tasking specific selectors to upstream Internet transaction collection.¹³¹ And, like other forms of Section 702 collection, selectors tasked for upstream Internet transaction collection must be specific selectors (such as an email address), and may not be key words or the names of targeted individuals.¹³²

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

¹²⁷ PCLOB March 2014 Hearing Transcript, *supra*, at 26 (statement of Rajesh De, General Counsel, NSA); *id.* at 51-53 (statement of Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ).

¹²⁸ NSA DCLPO REPORT, *supra*, at 6.

¹²⁹ PCLOB March 2014 Hearing Transcript, *supra*, at 53-54 (statements of Rajesh De, General Counsel, NSA, and Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ).

¹³⁰ Bates October 2011 Opinion, *supra*, at 15, 2011 WL 10945618, at *5.

¹³¹ NSA DCLPO REPORT, *supra*, at 5-6.

¹³² NSA DCLPO REPORT, *supra*, at 4; PCLOB March 2014 Hearing Transcript, *supra*, at 57 (statement of Rajesh De, General Counsel, NSA) (noting that a name cannot be tasked).

communications, what is referred to as the “Internet backbone.”¹³³ 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.¹³⁴

Upstream collection acquires Internet transactions that are “to,” “from,” or “about” a tasked selector.¹³⁵ With respect to “to” and “from” communications, the sender or a recipient is a user of a Section 702–tasked selector. This is not, however, necessarily true for an “about” communication. An “about” communication is one in which the tasked selector is referenced within the acquired Internet transaction, but the target is not necessarily a participant in the communication.¹³⁶ If the NSA therefore applied its targeting procedures to task email address “JohnTarget@example.com,” to Section 702 upstream collection, the NSA would potentially acquire communications routed through the Internet backbone that were sent from email address JohnTarget@example.com, that were sent to JohnTarget@example.com, and communications that mentioned JohnTarget@example.com in the body of the message. The NSA would not, however, acquire communications simply because they contained the name “John Target.” In a still-classified September 2008 opinion, the FISC agreed with the government’s conclusion that the government’s target when it acquires an “about” communication is not the sender or recipients of the communication, regarding whom the government may know nothing, but instead the targeted user of the Section 702–tasked selector. The FISC’s reasoning relied upon language in a congressional report, later quoted by the FISA Court of Review, that the

¹³³ The Intelligence Community’s Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3-4.

¹³⁴ Bates October 2011 Opinion, *supra*, at 73, 2011 WL 10945618, at *26.

¹³⁵ See, e.g., October 2011 Opinion, *supra*, at 15-16, 2011 WL 10945618, at *5-6 (describing the government’s representations regarding upstream collection in the first Section 702 certification the FISC reviewed).

¹³⁶ Bates October 2011 Opinion, *supra*, at 15, 2011 WL 10945618, at *5; Joint Statement of Lisa O. Monaco, Assistant Attorney General, National Security Division, Dept. of Justice, et. al., *Hearing Before the House Permanent Select Comm. on Intelligence: FISA Amendments Act Reauthorization*, at 7 (Dec. 8, 2011) (“December 2011 Joint Statement”) (statement of Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ), *available at* <http://www.dni.gov/files/documents/Joint%20Statement%20FAA%20Reauthorization%20Hearing%20-%20December%202011.pdf>; PCLOB March 2014 Hearing Transcript, *supra*, at 55.

“target” of a traditional FISA electronic surveillance “is the individual or entity . . . about whom or from whom information is sought.”¹³⁷

There are technical reasons why “about” collection is necessary to acquire even some communications that are “to” and “from” a tasked selector. In addition, some types of “about” communications actually involve Internet activity of the targeted person.¹³⁸ The NSA cannot, however, distinguish in an automated fashion between “about” communications that involve the activity of the target from communications that, for instance, merely contain an email address in the body of an email between two non-targets.¹³⁹

In order to acquire “about” communications while complying with Section 702’s prohibition on intentionally acquiring known domestic communications, the NSA is required to take additional technical steps that are not required for other Section 702 collection. 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.¹⁴⁰ If, for example, a person located in Chicago sent an email to a friend in Miami that mentioned the tasked selector “JohnTarget@example.com,” the IP filters (or comparable technical means) are designed to prevent the acquisition of this communication. The IP filters, however, do not operate perfectly,¹⁴¹ and may fail to filter out a domestic communication before it is screened against tasked selectors. A United States-based user, for example, may send a communication (intentionally or otherwise) via a foreign server even if the intended recipient is also in the United States.¹⁴² As such, the FISC has noted the government’s concession that in the ordinary course of acquiring single communications, wholly domestic communications could be acquired as much as 0.197% of the time.¹⁴³ While this percentage is small, the FISA court estimated in 2011 that the

¹³⁷ See *In re Sealed Case*, 310 F.3d 717, 740 (FISA Ct. Rev. 2002) (quoting H.R. Rep. 95-1283, at 73 (1978)); see also PCLOB March 2014 Hearing Transcript, *supra*, at 55 (statement of Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ) (confirming the FISC had held that targeting includes communications about a particular selector that are not necessarily to or from that selector).

¹³⁸ Bates October 2011 Opinion, *supra*, at 37-38, 2011 WL 10945618, at *12 (describing the types of acquired Internet transactions and noting that a subset involve transactions of the target).

¹³⁹ Bates October 2011 Opinion, *supra*, at 31, 43, 2011 WL 10945618, at *10, *14 (describing limitations on what can be distinguished at the acquisition stage).

¹⁴⁰ Bates October 2011 Opinion, *supra*, at 33, 2011 WL 10945618, at *11 (regarding the “technical measures” that NSA uses to prevent the acquisition of upstream collection of domestic communications); NSA DCLPO REPORT, *supra*, at 5-6 (acknowledging that IP filters are used to prevent the acquisition of domestic communications).

¹⁴¹ December 2011 Joint Statement, *supra*, at 7 (acknowledging measures to prevent acquisition of domestic communications “are not perfect”).

¹⁴² Bates October 2011 Opinion, *supra*, at 34-35 n.33, 2011 WL 10945618, at *11 n.33.

¹⁴³ Bates October 2011 Opinion, *supra*, at 34 n.32, 2011 WL 10945618, at *11 n.32.

overall number of communications the government acquires through Section 702 upstream collection could result in the government acquiring as many as tens of thousands of wholly domestic communications per year.¹⁴⁴

In addition, wholly domestic communications could also be acquired because they were embedded in a larger multi-communication transaction (“MCT”), the subject of the next section.

3. Upstream Collection of Internet Communications: Multi-Communication Transactions (“MCTs”)

While the NSA’s upstream collection is intended to acquire Internet *communications*, it does so through the acquisition of Internet *transactions*. The difference between *communications* and *transactions* is a significant one, and the government’s failure to initially distinguish and account for this distinction caused the FISA court to misunderstand the nature of the collection for over two years, and later to find a portion of the Section 702 program to be unconstitutional.

The NSA-designed upstream Internet collection devices acquire transactions as they cross the Internet. An Internet transaction refers to any set of data that travels across the Internet together such that it may be understood by a device on the Internet.¹⁴⁵ An Internet transaction could consist of a single discrete communication, such as an email that is sent from one server to another. Such communications are referred to as single communication transactions (SCTs).¹⁴⁶ Of the upstream Internet transactions that the NSA acquired in 2011, approximately ninety percent were SCTs.¹⁴⁷

In other instances, however, a single Internet transaction might contain multiple discrete communications. These transactions are referred to as MCTs.¹⁴⁸ If a single discrete communication within an MCT is to, from, or about a Section 702–tasked selector, and at least one end of the transaction is foreign, the NSA will acquire the entire MCT.¹⁴⁹

If the acquired MCT is a transaction between the Section 702 target (who is assessed to be a non-U.S. person located outside the United States and is targeted to acquire foreign intelligence information falling under one of the approved certifications) and a server, then

¹⁴⁴ Bates October 2011 Opinion, *supra*, at 34 n.32, 2011 WL 10945618, at *11 n.32; December 2011 Joint Statement, *supra*, at 7.

¹⁴⁵ See Bates October 2011 Opinion, *supra*, at 28 n.23, 2011 WL 10945618, at *9 n.23 (quoting government characterization of what constitutes an Internet transaction).

¹⁴⁶ Bates October 2011 Opinion, *supra*, at 27-28, 2011 WL 10945618, at *9.

¹⁴⁷ Bates October 2011 Opinion, *supra*, at 34 n.32, 2011 WL 10945618, at *11 n.32.

¹⁴⁸ Bates October 2011 Opinion, *supra*, at 28, 2011 WL 10945618, at *9.

¹⁴⁹ December 2011 Joint Statement, *supra*, at 7.

all of the discrete communications acquired within the MCT are also communications to or from the target. Based on a statistical sample conducted by the NSA, the FISC estimated that as of 2011 the NSA acquired between 300,000 and 400,000 such MCTs every year (i.e., MCTs where the “active user,”¹⁵⁰ was the target him or herself).¹⁵¹

When the acquired MCT is not a transaction between the target and the server, but instead a transaction between another individual and a server that happens to include a Section 702 tasked selector, the MCT may “include communications that are not about a tasked selector and may have no relationship, or no more than an incidental relationship to the [tasked] selector.”¹⁵² These non-target MCTs break down into three categories. Based on the NSA’s statistical study, the FISC estimated that (as of 2011) the NSA acquired at least 1.3 million MCTs each year where the user who caused the transaction to occur was not the target, but was located outside the United States.¹⁵³ Using this same statistical analysis, the FISA court estimated that the NSA would annually acquire an additional approximately 7,000 to 8,000 MCTs of non-targeted users who were located in the United States, and between approximately 97,000 and 140,000 MCTs each year where NSA would not be able to determine whether the user who caused the transaction to occur was located inside or outside the United States.¹⁵⁴

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.”¹⁵⁵ While some distinction between SCTs and MCTs can be made with respect to some communications in conducting acquisition, the government has not been able to design a filter that would acquire only the single discrete communications within transactions that contain a Section 702 selector. This is due to the constant changes in the protocols used by Internet service providers and the services provided.¹⁵⁶ If time

¹⁵⁰ The “active user” is the actual human being who is interacting with a server to engage in an Internet transaction.

¹⁵¹ Bates October 2011 Opinion, *supra*, at 38, 2011 WL 10945618, at *12.

¹⁵² December 2011 Joint Statement, *supra*, at 7.

¹⁵³ Bates October 2011 Opinion, *supra*, at 39, 2011 WL 10945618, at *12.

¹⁵⁴ Bates October 2011 Opinion, *supra*, at 38-40, 2011 WL 10945618, at *12. With respect to this last category, the unidentified user could be the Section 702 target. *Id.* at 38, 40-41, 2011 WL 10945618, at *12.

¹⁵⁵ Bates October 2011 Opinion, *supra*, at 31, 2011 WL 10945618, at *10. In 2011, the NSA was able to determine that approximately 90 percent of all upstream Internet transactions consisted of SCTs as the result of a post-acquisition statistical sample that required a manual review. *Id.* at 34 n.32, 2011 WL 10945618, at *11.

¹⁵⁶ Bates October 2011 Opinion, *supra*, at 32, 2011 WL 10945618, at *10.

were frozen and the NSA built the perfect filter to acquire only single, discrete communications, that filter would be out-of-date as soon as time was restarted and a protocol changed, a new service or function was offered, or a user changed his or her settings to interact with the Internet in a different way. Conducting upstream Internet acquisition will therefore continue to result in the acquisition of some communications that are unrelated to the intended targets.

The fact that the NSA acquires Internet communications through the acquisition of Internet transactions, be they SCTs or MCTs, has implications for the technical measures, such as IP filters, that the NSA employs to prevent the intentional acquisition of wholly domestic communications. With respect to SCTs, wholly domestic communications that are routed via a foreign server for any reason are susceptible to Section 702 acquisition if the SCT contains a Section 702 tasked selector.¹⁵⁷ With respect to MCTs, wholly domestic communications also may be embedded within Internet transactions that also contain foreign communications with a Section 702 target. The NSA's technical means for filtering domestic communications cannot currently discover and prevent the acquisition of such MCTs.¹⁵⁸

Because of the greater likelihood that upstream collection of Internet transactions, in particular MCTs, will result in the acquisition of wholly domestic communications and extraneous U.S. person information, there are additional rules governing the querying, retention, and use of such upstream data in the NSA minimization procedures. These additional procedures are discussed below.

IV. Targeting Procedures: Who May Be Targeted? How? And Who Decides?

As is discussed above, the government targets persons under Section 702 by tasking selectors — communication facilities, such as email addresses and telephone numbers — that the government assesses will be used by those persons to communicate or receive foreign intelligence information that falls within one of the authorized Section 702 certifications.¹⁵⁹ Under Section 702, this targeting process to determine which persons are (1) non-U.S. persons, that are (2) reasonably believed to be located outside the United States, who will (3) use the tasked selectors to communicate or receive foreign intelligence

¹⁵⁷ Bates October 2011 Opinion, *supra*, at 34-35, n.32 & n.33; *id.* at 45, 2011 WL 10945618, at *11 (“[T]he 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.”)

¹⁵⁸ Bates October 2011 Opinion, *supra*, at 45, 47, 2011 WL 10945618, at *15.

¹⁵⁹ *See, e.g.*, AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-2.

information is governed by targeting procedures.¹⁶⁰ While the targeting procedures are subject to judicial review by the FISC,¹⁶¹ individual targeting determinations made under these targeting procedures are not reviewed by the FISC (but are subject to internal Executive oversight, as detailed below).¹⁶²

Both the NSA and FBI have targeting procedures that govern the process by which persons may be targeted under Section 702.¹⁶³ While some information has been released by the government, neither the NSA nor the FBI targeting procedures have been declassified in full. The NSA's Section 702 targeting procedures take primary importance because only the NSA may initiate Section 702 collection.¹⁶⁴ The FBI's Section 702 targeting procedures, which are discussed further below, are applied to certain selectors only after the NSA has previously determined under the NSA targeting procedures that these selectors qualify for Section 702 targeting.¹⁶⁵ Although the NSA initiates all Section 702 targeting, and thus makes all initial decisions pursuant to its targeting procedures regarding whether a person qualifies for Section 702 targeting under one of the Section 702 certifications, the CIA and FBI have processes to "nominate" targets to the NSA for Section 702 targeting.¹⁶⁶ It is the NSA, however, that must make the determination whether to initiate targeting.

Section 702 targeting begins when an NSA analyst discovers or is informed of a foreign intelligence lead — specifically, information indicating that a particular person may possess or receive the types of foreign intelligence information described within one of the Section 702 certifications.¹⁶⁷ Lead information could come from any of multiple sources, including human intelligence, signals intelligence or other sources such as law enforcement information. Because Section 702 acquisition is selector-based, the NSA analyst must also

¹⁶⁰ See 50 U.S.C. § 1881a(d)(1) (requirement for targeting procedures); AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-1 (general scope of what is covered by those targeting procedures).

¹⁶¹ 50 U.S.C. § 1881a(d)(2).

¹⁶² NSA DCLPO REPORT, *supra*, at 2, 4-5.

¹⁶³ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 6, 9.

¹⁶⁴ See The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3 (noting that "NSA takes the lead in targeting and tasks both telephone and electronic communications selectors to acquire communications"); AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 6 ("[A]ll Section 702 targeting is initiated pursuant to the NSA's targeting procedures.").

¹⁶⁵ The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3.

¹⁶⁶ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-8, A-12.

¹⁶⁷ NSA DCLPO REPORT, *supra*, at 4.

discover or be informed of a specific selector used by this potential target that could be tasked to PRISM and/or upstream collection.¹⁶⁸

Having identified a potential person to target through the tasking of a selector, the NSA analyst must then apply the targeting procedures. These procedures require the NSA analyst to make a determination regarding the assessed location and non-U.S. person status of the potential target (the *foreignness determination*)¹⁶⁹ and whether the target possesses and/or is likely to communicate or receive foreign intelligence information authorized under an approved certification (the *foreign intelligence purpose determination*).¹⁷⁰

A. Foreignness Determination

With respect to the *foreignness determination*, the NSA analyst is required to assess whether the target of the acquisition is a non-U.S. person reasonably believed to be located outside the United States based upon the totality of the circumstances available.¹⁷¹ This analysis begins with a review of the initial lead information, which must be examined to determine whether it indicates either the location or the U.S. person status of the potential target.¹⁷² At times, the lead information itself will state where the target is assessed to be located and their U.S. person status. In other instances, this information may only enable an analyst to infer location or U.S. person status. In either case, the Section 702 targeting determination may not be made upon the lead information alone. Instead, the NSA analyst must check multiple sources and make a determination based on the totality of the circumstances available to the analyst.¹⁷³

The government has stated that in making this foreignness determination the NSA targeting procedures inherently impose a requirement that analysts conduct “due diligence” in identifying these relevant circumstances. What constitutes due diligence will

¹⁶⁸ NSA DCLPO REPORT, *supra*, at 4.

¹⁶⁹ PCLOB March 2014 Hearing Transcript, *supra*, at 41 (statement of Rajesh De, General Counsel, NSA) (stating that “foreignness determination” is a “shorthand for referring to the determination that [the target] is a non-U.S. person reasonably located to be abroad”).

¹⁷⁰ PCLOB March 2014 Hearing Transcript, *supra*, at 61 (statement of Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ) (describing individualized foreign intelligence purpose determination which must be documented as part of the tasking process).

¹⁷¹ NSA DCLPO REPORT, *supra*, at 4; PCLOB March 2014 Hearing Transcript, *supra*, at 42 (statement of Rajesh De, General Counsel, NSA) (noting that foreignness determination is a “totality of the circumstances” test).

¹⁷² The Intelligence Community’s Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3.

¹⁷³ NSA DCLPO REPORT, *supra*, at 4; PCLOB March 2014 Hearing Transcript, *supra*, at 41 (statement of Rajesh De, General Counsel, NSA) (in describing foreignness determination, stating that “an analyst must take into account all available information. . . [A]n analyst cannot ignore any contrary information to suggest that that is not the correct status of the person.”)

vary depending on the target; tasking a new selector used by a foreign intelligence target with whom the NSA is already quite familiar may not require deep research into the target's (already known) U.S. person status and current location, while a great deal more effort may be required to target a previously unknown, and more elusive, individual. As previously discussed above, a failure by an NSA analyst to conduct due diligence in identifying relevant circumstances regarding the location and U.S. person status of a Section 702 target is a reportable compliance incident to the FISC.

After conducting due diligence and reviewing the totality of the circumstances, the NSA analyst is required to determine whether the information indicates that the target is a non-U.S. person reasonably believed to be located outside the United States.¹⁷⁴ The government has stated, and the Board's review has confirmed, that this is not a "51% to 49% test."¹⁷⁵ If there is conflicting information indicating whether a target is located in the United States or is a U.S. person, that conflict must be resolved and the user must be determined to be a non-U.S. person reasonably believed to be located outside the United States prior to targeting.¹⁷⁶

While conflicting information must be resolved, the standard for making the foreignness determination is not a probable cause standard. Through the application of the NSA targeting procedures over the years and interactions with and between and among NSA personnel and external DOJ/Office of the Director of National Intelligence ("ODNI") overseers, a common understanding has been developed regarding what constitutes a sufficient basis for determining that a potential Section 702 target is a non-U.S. person reasonably believed to be located outside the United States. The NSA targeting procedures include a process for assessing non-U.S. person's status. This determination may not be made unless the analyst has first undertaken due diligence.

In 2013, the DOJ undertook a review designed to assess how often the foreignness determinations that the NSA made under the targeting procedures as described above turned out to be wrong — i.e., how often the NSA tasked a selector and subsequently realized after receiving collection from the provider that a user of the tasked selector was either a U.S. person or was located in the United States. The DOJ reviewed one year of data and determined that 0.4% of NSA's targeting decisions resulted in the tasking of a selector that, as of the date of tasking, had a user in the United States or who was a U.S. person. As is discussed in further detail below, data from such taskings in most instances must be

¹⁷⁴ See PCLOB March 2014 Hearing Transcript, *supra*, at 40-42 (statement of Rajesh De, General Counsel, NSA).

¹⁷⁵ PCLOB March 2014 Hearing Transcript, *supra*, at 40-41 (statement of Rajesh De, General Counsel, NSA).

¹⁷⁶ NSA DCLPO REPORT, *supra*, at 4; PCLOB March 2014 Hearing Transcript, *supra*, at 40-42 (statement of Rajesh De, General Counsel, NSA).

purged. The purpose of the review was to identify how often the NSA's foreignness determinations proved to be incorrect. Therefore, the DOJ's percentage does not include instances where the NSA correctly determined that a target was located outside the United States, but post-tasking, the target subsequently traveled to the United States.

B. Foreign Intelligence Purpose Determination

In addition to the foreignness determination, the NSA analyst must also make a *foreign intelligence purpose determination*. Specifically, the NSA targeting procedures require that the NSA determine that tasking the selector will be likely to acquire one of the types of foreign intelligence information identified in a Section 702 certification.¹⁷⁷ In making this determination, the NSA analyst must identify the specific foreign power or foreign territory concerning which the foreign intelligence information is being sought.¹⁷⁸ The NSA targeting procedures include a non-exclusive list of factors that the NSA will consider in determining whether the tasking of a selector will be likely to result in foreign intelligence information falling within one of the Section 702 certifications.

C. Documentation Requirements

The NSA targeting procedures contain documentation requirements with respect to aspects of the foreignness and foreign intelligence purpose determinations. Analysts are required under the NSA targeting procedures to cite the specific documents and communications that led them to assess that the Section 702 target is located outside the United States.¹⁷⁹ As a practical matter, these citations are accompanied by a narrative explaining what the documents and communications indicate with regard to the location of the target. In other words, with respect to the determination regarding the location of the target, analysts must "show their work." Although analysts are required under the targeting procedures to conduct an analysis regarding why the targeting of the individual will result in obtaining foreign intelligence information under the Section 702 certifications, analysts are not required to document (i.e., show their work) this foreign intelligence purpose determination in the same manner as they are required to document the foreignness determination. With respect to the foreign intelligence purpose, the NSA targeting procedures require the analyst only to "identify" the foreign power or foreign territory regarding which the foreign intelligence information is to be acquired.¹⁸⁰ By policy, but not as a requirement of the targeting procedures, the NSA also requires that all taskings be accompanied by a very brief statement (typically no more than one sentence

¹⁷⁷ NSA DCLPO REPORT, *supra*, at 4.

¹⁷⁸ See AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-5 (noting that the identified foreign power or foreign territory must be documented).

¹⁷⁹ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-5; see also NSA DCLPO REPORT, *supra*, at 4-5.

¹⁸⁰ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-5.

long) that further explains the analyst's rationale for assessing that tasking the selector in question will result in the acquisition of the types of foreign intelligence information authorized by the Section 702 certifications.¹⁸¹

In the Board's view, this reduced documentation regarding the foreign intelligence purpose determination results in a less rigorous review by the NSA's external overseers of the foreign intelligence purpose determinations than the NSA's foreignness determination. Also as a matter of NSA policy, as opposed to a requirement in the NSA targeting procedures, NSA analysts document the assessed non-U.S. person status of the target, but analysts do not separately document the basis for this non-U.S. person determination. In general, however, the non-U.S. person analysis is based upon same information that underlies the determination regarding the target's location.

D. Approvals

Once analysts have documented their determinations in an NSA tasking database,¹⁸² the tasking request undergoes two layers of review before actual Section 702 acquisition is initiated.¹⁸³ Two different senior NSA analysts must review the documentation accompanying the tasking request to ensure that it meets all of the requirements of the NSA targeting procedures.¹⁸⁴ Both NSA senior analysts receive additional training to review tasking requests.¹⁸⁵ Both senior analysts may also request additional information prior to approving or denying the Section 702 tasking request.¹⁸⁶ Both senior analysts are required to review all aspects of the tasking before approving the tasking request.¹⁸⁷

Once the tasking request receives all of the necessary approvals, it is sent to one or more electronic communication service providers that have received a Section 702 directive in order to initiate Section 702 acquisition.¹⁸⁸ The tasking request, however, is subjected to further post-tasking review by the DOJ/ODNI review team,¹⁸⁹ as is discussed in the "External Oversight" section below.

¹⁸¹ See generally PCLOB March 2014 Hearing Transcript, *supra*, at 59 (statement of Rajesh De, General Counsel, NSA) (discussing foreign intelligence purpose determination and noting that it must be "documented in a targeting rationale document").

¹⁸² August 2013 Semiannual Assessment, *supra*, at A-5.

¹⁸³ NSA DCLPO REPORT, *supra*, at 5.

¹⁸⁴ NSA DCLPO REPORT, *supra*, at 5.

¹⁸⁵ NSA DCLPO REPORT, *supra*, at 5.

¹⁸⁶ NSA DCLPO REPORT, *supra*, at 5.

¹⁸⁷ NSA DCLPO REPORT, *supra*, at 5.

¹⁸⁸ NSA DCLPO REPORT, *supra*, at 5.

¹⁸⁹ NSA DCLPO REPORT, *supra*, at 5; AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 6-7.

E. CIA and FBI Nominations

The CIA and FBI have both developed processes to nominate selectors to the NSA to be tasked for Section 702 acquisition.¹⁹⁰ The NSA evaluates the CIA and FBI nominations under the same targeting procedures and using the same processes that are described above. It is the NSA that is ultimately responsible for the tasking of such facilities. In order to ensure that the NSA's foreignness and foreign intelligence purpose determinations regarding the CIA and FBI nominations are made on accurate and current information, both the CIA and FBI have implemented internal requirements prior to formally nominating a selector to the NSA for acquisition. For example, the CIA nominations are reviewed and approved by the targeting officer's first line manager, a legal officer, a senior operational manager, and the CIA's FISA Program office prior to being exported to the NSA.¹⁹¹ These internal procedures are in addition to the NSA documentation and approval requirements required for all taskings.

F. FBI Targeting Procedures

The FBI's targeting procedures govern certain aspects of the PRISM program; specifically, requests for certain communications for selectors that have already been determined by the NSA to have met its targeting procedures. As the NSA has already made a foreignness determination with respect to any selector for which the FBI will be acquiring communications, the FBI's role in targeting is substantially different than that of the NSA.¹⁹² Instead of establishing the required information to indicate that a Section 702 target is a non-U.S. person reasonably believed to be located outside the United States who is likely to communicate or receive foreign intelligence information, the FBI targeting procedures are intended to "provide additional assurance that the users of tasked accounts are non-United States persons located outside the United States."¹⁹³ The FBI targeting procedures therefore require the FBI to both review the NSA's foreignness determinations¹⁹⁴ and review information available to the FBI. FBI personnel who process tasking requests receive training in both the FBI targeting procedures and a detailed set of standard operating procedures that describe the steps that the FBI must take to ensure that they

¹⁹⁰ See *supra* footnote 1664 and accompanying text.

¹⁹¹ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-8; see also AUGUST 2013 SEMIANNUAL ASSESSMENT at 36 (describing compliance incident related to an FBI nomination that stemmed from reliance on an unsupported fact).

¹⁹² The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3.

¹⁹³ Bates October 2011 Opinion, *supra*, at 22, 2011 WL 10945618, at *7.

¹⁹⁴ The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3.

have conducted due diligence in looking for information that may alter or affect the NSA's foreignness assessment.¹⁹⁵

V. Post-Tasking Review and Related Reporting and Purging Requirements

In addition to defining the process by which Section 702 tasking will be initiated, the NSA targeting procedures also impose additional post-tasking requirements designed to ensure that the users of tasked selectors remain non-U.S. persons located outside the United States and that acquisition against the selector continues only insofar as the government assesses that the tasking is likely to acquire foreign intelligence information within one of the authorized Section 702 certifications. The manner in which the post-tasking checks required by the NSA targeting procedures will be implemented has been supplemented by additional filings by the government with the FISC. The government has reported to the FISA court and Congress as compliance incidents instances in which its implementation of the required post-tasking checks did not correspond with these additional representations to the court.

NSA analysts are required to routinely review at least a sample of the Section 702-acquired communications for selectors that they have tasked to ensure that the selectors remain properly tasked.¹⁹⁶ The NSA has developed automated systems to remind analysts to review collection from email addresses and comparable selectors within five business days after the first instance that data is acquired for a particular tasked selector, and at least every 30 days thereafter; comparable systems have to-date not been implemented with respect to Section 702 acquisition of upstream telephony collection. The analysts review the content to verify that the selector is associated with the foreign intelligence target, as well as look for any information indicating that a user of the selector is a U.S. person or located in the United States.¹⁹⁷ The NSA also requires analysts to re-verify at least once a year that each selector continues to be tasked in order to acquire the types of foreign intelligence information specified in the certification under which the selector is tasked. The CIA and FBI have each implemented their own comparable policies and practices mandating that analysts, agents, and officers initially review and periodically verify data acquired from selectors nominated by the CIA and FBI to ensure the selectors remain properly tasked for Section 702 acquisition.

¹⁹⁵ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 36, A-11 to A-12.

¹⁹⁶ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-4; NSA DCLPO REPORT, *supra*, at 6.

¹⁹⁷ NSA DCLPO REPORT, *supra*, at 6; *see also* PCLOB March 2014 Hearing Transcript, *supra*, at 42 (statement of Rajesh De, General Counsel, NSA) (noting that “analysts have an affirmative obligation to periodically revisit the foreignness determination”)

In addition to this content review, the NSA is required to conduct routine post-tasking checks of all Section 702–tasked selectors.¹⁹⁸

If it is determined that a user of a tasked selector is either in the United States or is a U.S. person, the selector is required to be promptly detasked from Section 702 acquisition (i.e., all Section 702 acquisition directed at that selector must be terminated).¹⁹⁹ Any other Section 702–tasked selectors assessed to be used by the individual determined to be a U.S. person or located in the United States must also be promptly detasked.²⁰⁰ Additionally, selectors must be detasked if the government determines that it will not obtain the types of foreign intelligence information authorized under the Section 702 certifications.²⁰¹ Failure to detask a selector from Section 702 acquisition after it has been (or, based on the available information, should have been) determined to be ineligible for further Section 702 acquisition is a compliance incident that must be reported first to the DOJ and ODNI, and in turn to the FISC and Congress.²⁰²

If it is learned that a tasked selector is being used by a U.S. person or person located in the United States, the data acquired from the selector while it was being used by the U.S. person or person located in the United States is subject to purge, with limited exceptions.²⁰³ If the data was acquired as a result of a compliance incident — because, for example, there was an error in the tasking (e.g., typographical error, lack of due diligence tasking, etc.); an error in detasking (insufficiently prompt detasking); or an overproduction by the provider — the acquired communications must be purged.²⁰⁴ In cases where there is no underlying compliance incident but a user is determined to be a U.S. person or a person located in the United States (e.g., the government had a reasonable, but ultimately mistaken, belief that a target was located outside the United States), a purge of acquired communications is also required.²⁰⁵

¹⁹⁸ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 6.

¹⁹⁹ NSA DCLPO REPORT, *supra*, at 6; *see also* NSA October 2011 Minimization Procedures, *supra*, § 3(d)(1).

²⁰⁰ NSA DCLPO REPORT, *supra*, at 6; *see also* NSA October 2011 Minimization Procedures, *supra*, § 3(d)(1).

²⁰¹ NSA DCLPO REPORT, *supra*, at 6.

²⁰² *See* AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 7 (noting that the NSA must report all instances in which a target is found to be located in the United States, but that such incidents are only compliance incidents if the NSA “knew or should have known the target was in the United States during the collection period”); *id.* at 25-27, 29, 33 (describing the category of detasking incidents and specific detasking incidents); NSA DCLPO REPORT, *supra*, at 3 (summarizing reporting process).

²⁰³ NSA DCLPO REPORT, *supra*, at 8.

²⁰⁴ *See, e.g.*, PCLOB March 2014 Hearing Transcript, *supra*, at 72.

²⁰⁵ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-12 (noting that all of the agency minimization procedures require purges when a target is discovered to be a U.S. person or person located in the United States, with limited exceptions).

Certain exceptions apply, however, in instances where the communications were not acquired as the result of a violation of the targeting or minimization procedures. The NSA minimization procedures permit the Director (or Acting Director) of the NSA to waive, on a communication-by-communication basis, specific communications determined to contain “significant foreign intelligence information” or information that is not foreign intelligence information but is “evidence of a crime.”²⁰⁶ The CIA and FBI standards for executing a waiver are similar. Additionally, and notwithstanding the general purge requirement and the specific waiver exceptions, the NSA may also inform the FBI that a target has entered the United States so that the FBI make seek traditional FISA electronic surveillance of the target or take other lawful investigative steps.²⁰⁷ The NSA may also retain and disclose to the FBI and CIA certain technical data for collection avoidance purposes.²⁰⁸

VI. Minimization and Related Requirements: What Are the Limitations Regarding How the Data is Acquired, Who May View It, How Long It Is Retained, and with Whom It May be Shared?

Minimization is one of the most confusing terms in FISA. Like traditional FISA electronic surveillance and physical search,²⁰⁹ Section 702 requires that all acquired data be subject to “minimization procedures.”²¹⁰ Minimization procedures are best understood as a set of controls on data to balance privacy and national security interests. Specifically, under FISA, minimization procedures must be “specific procedures . . . that are reasonably designed in light of the purpose and technique of the particular surveillance *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.*”²¹¹ Minimization procedures must also contain special limitations on the dissemination of U.S.

²⁰⁶ NSA October 2011 Minimization Procedures, *supra*, § 5(1) and (2). The NSA’s minimization procedures also allow for the Director of the NSA to waive the purge of a communication that is assessed to contain “technical data base information,” “information necessary to understand or assess a communications security vulnerability,” or “information pertaining to a threat of serious harm to life or property.” NSA October 2011 Minimization Procedures § 5(3), (4). To date, no waivers have been granted under these additional provisions.

²⁰⁷ NSA October 2011 minimization procedures, *supra*, § 5.

²⁰⁸ NSA October 2011 minimization procedures, *supra*, § 5.

²⁰⁹ See 50 U.S.C. §§ 1805(a)(3) and 1824(a)(3).

²¹⁰ 50 U.S.C. § 1881a(e).

²¹¹ 50 U.S.C. 1801(h)(1) (emphasis added).

person identities with respect to certain types of foreign intelligence information,²¹² as well as allow for the retention and dissemination of evidence of a crime to law enforcement entities.²¹³ These statutory requirements obligate the Attorney General to adopt procedures that balance the at times competing interests in protecting the privacy of U.S. persons and the Intelligence Community's production of foreign intelligence information to meet national security requirements. In addition, although the minimization procedures must be designed to protect U.S. persons' privacy, the procedures will at times provide controls on data that protect the privacy of non-U.S. persons as well.

This section describes the controls imposed by the Section 702 minimization procedures on acquisition, access (and related training requirements), querying, retention (and purging), and dissemination. The NSA's 2011 Section 702 minimization procedures have been publicly released.²¹⁴ Minimization procedures for the CIA, FBI, and National Counterterrorism Center ("NCTC")²¹⁵ have not been publicly released to date, though some information regarding these procedures has been declassified. Although the minimization procedures for each agency have many similarities, there are differences between the agencies' minimization procedures that are related to the different authorities of the respective agencies and the way each uses the Section 702-acquired data.²¹⁶ Some of these differences impact privacy concerns.

All Section 702-acquired data, both content and metadata, is subject to the Section 702 minimization procedures.²¹⁷

A. Acquisition

The minimization procedures of agencies that conduct acquisition — in the case of Section 702, the NSA and FBI — must contain provisions that minimize the acquisition of U.S. person information consistent with the authorized purpose of the collection. The first minimization of the acquisition of U.S. person information, however, stems from the targeting requirements imposed by the statute itself. As an initial matter, Section 702

²¹² 50 U.S.C. § 1801(h)(2) (further limiting dissemination of U.S. person identities with regard to foreign intelligence information as defined by § 1801(e)(2), but not § 1801(e)(1)).

²¹³ 50 U.S.C. § 1801(h)(3).

²¹⁴ See NSA 2011 Minimization Procedures, *supra*, available at <http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf>.

²¹⁵ As described below, the NCTC's role in processing and minimizing Section 702 data is limited. See AUGUST 2013 JOINT ASSESSMENT, *supra*, at 4 n.2.

²¹⁶ PCLOB March 2014 Hearing Transcript, *supra*, at 18-19 (discussion between David Medine, Chairman, PCLOB, and Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ).

²¹⁷ PCLOB March 2014 Hearing Transcript, *supra*, at 19.

prohibits the intentional targeting of U.S. persons, the intentional targeting of persons located in the United States, reverse targeting, or the intentional acquisition of communications known to be wholly domestic at the time of acquisition.²¹⁸ Each of these statutory requirements is designed to reduce, though not eliminate, the acquisition of U.S. person information.

The NSA minimization procedures therefore start with a requirement that Section 702 collection be conducted in accordance with the Section 702 certification, and “in a manner designed, to the greatest extent reasonably feasible, to minimize the acquisition of information not relevant to the authorized purpose.”²¹⁹ This mandate applies to both the NSA’s acquisition and the technical assistance provided by the FBI in acquiring communications.²²⁰ Affidavits accompanying the certifications, witness testimony in hearings before the FISC, and additional filings before the court describe how the NSA and FBI will actually conduct the acquisition in a manner that the government believes will be reasonably designed to minimize the acquisition of information that is irrelevant to the acquisition of the foreign intelligence information specified in the Section 702 certifications.²²¹ These representations detail the method and techniques by which the collection of PRISM and upstream collection is conducted, as described above. A failure to implement the acquisition in a manner that reasonably limits the collection to the authorized purpose of the Section 702 certifications can, and has, led to incidents of noncompliance with the minimization procedures that have been reported to the FISC and Congress.²²²

In addition to actually acquiring the data, certain technical actions must be undertaken at or just after the acquisition stage in order to facilitate later compliance with other minimization rules. For example, data-tagging Section 702-acquired data at, or just after, acquisition is also employed to effectuate other access and routing controls, certain

²¹⁸ 50 U.S.C. § 1881a(a), (b).

²¹⁹ NSA October 2011 Minimization Procedures, *supra*, § 3(a).

²²⁰ See NSA October 2011 Minimization Procedures, *supra*, § 2(a) (defining “acquisition” as “the collection by NSA or the FBI through electronic means of a non-public communication to which it is not an intended party”).

²²¹ See, e.g., Bates October 2011 Opinion, *supra*, at 5-10, 2011 WL 10945618, at *2-3 (describing various government submissions regarding how the government conducts Section 702 upstream collection); *id.* at 15-16, 2011 WL 10945618, at *5 (describing comparable descriptions in prior dockets); *id.* at 29-41, 2011 WL 10945618, at *9-13 (further describing government descriptions regarding how the government conducts Section 702 upstream collection).

²²² See AUGUST 2013 SEMI-ANNUAL ASSESSMENT, *supra*, at 31 (describing “compliance incidents during this reporting period [that] resulted in NSA’s systems overcollecting data beyond what was authorized under the Section 702 certifications”).

controls limiting the scope of queries, and age-off and purge requirements. Each of these controls is discussed further below.

B. Access and Training

Although the minimization process begins with acquisition, FISA-acquired data that has yet to be reviewed and evaluated by a human being is still referred to by the government as being “unminimized” or “raw” data. The NSA, CIA, and FBI are the three Intelligence Community agencies that have access to such unminimized Section 702–acquired data.²²³ Each agency limits access to unminimized Section 702–acquired data to personnel who have been trained to apply their respective agency’s minimization procedures. To enforce these restrictions, all unminimized Section 702–acquired data must be stored in repositories with access controls designed to prevent unauthorized access of the data by those within or outside of the relevant agency.

The NSA’s core access and training requirements are found in the NSA’s targeting procedures, which have not been released to the public. NSA analysts are required to undergo mandatory training and must pass a test regarding the requirements of the Section 702 minimization procedures (among other legal requirements) prior to receiving access to unminimized Section 702–acquired data.²²⁴

The CIA’s minimization procedures similarly limit access to unminimized Section 702–acquired data to analysts who have received training in the CIA minimization procedures.²²⁵ The CIA conducts in-person training regarding its minimization procedures before its personnel receive access to Section 702 data repositories and also embeds FISA-trained attorneys with CIA personnel to answer questions on the application of those minimization procedures to actual collection.²²⁶

The FBI has created a mandatory online training course that must be taken before FBI agents or analysts are granted access to repositories of unminimized Section 702–acquired data.²²⁷ The Department of Justice’s National Security Division (“NSD”) and the FBI also conduct in-person trainings at FBI field offices.²²⁸

²²³ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-12.

²²⁴ NSA DCLPO REPORT, *supra*, at 4.

²²⁵ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-9.

²²⁶ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-9.

²²⁷ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 14 and A-12; *see also* PCLOB March 2014 Hearing Transcript at 86 (statement of James A. Baker, General Counsel, FBI) (confirming that access controls exists for FBI systems holding Section 702–acquired data).

²²⁸ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 14.

When an analyst, agent, or officer is granted access to unminimized Section 702–acquired data after receiving the requisite training, this does not mean that the agent or analyst has access to all such data. Agencies separate acquired data as a security measure. Furthermore, the CIA and FBI do not have copies of all Section 702–acquired data as neither agency receives all PRISM data acquired by the NSA, nor does either agency receive upstream collection.²²⁹

In addition to these general access and training requirements, the NSA’s minimization procedures impose supplemental requirements with respect to certain Internet transactions. When the “active user” (i.e., the actual human being who is interacting with a server to engage in an Internet transaction) associated with an MCT is either reasonably believed to be located in the United States, or when the NSA cannot determine where the active user is located, the NSA must segregate the MCT in a special access-controlled repository.²³⁰ Only analysts who have been trained in how to review such communications to identify any wholly domestic communications within such MCTs are permitted access to this repository.²³¹ A multi-communication transaction may not be moved out of the special-access repository or otherwise used unless it has been determined that none of the discrete communications that make up the MCT are wholly domestic communications.²³² If an MCT within this repository is determined to contain a wholly domestic communication, it must be destroyed upon recognition.²³³ The CIA and FBI do not have access to any unminimized Section 702–acquired upstream collection.²³⁴

Separately, certain access and training requirements are imposed by the NCTC’s Section 702 minimization procedures. The NCTC does not have access to unminimized Section 702–acquired data.²³⁵ The NCTC has, however, been provided access to certain FBI systems that contain Section 702–acquired data that has been minimized to meet the FBI’s dissemination standard. Minimization in this context means that any nonpublicly available Section 702–acquired U.S. person information in these FBI systems has been determined to either to be foreign intelligence information, necessary to understand or assess the importance of foreign intelligence information, or evidence of a crime.²³⁶ U.S. person information that is evidence of a crime but is not otherwise foreign intelligence

²²⁹ Bates October 2011 Opinion, *supra*, at 18 n.17, 2011 WL 10945618, at *6 n.17.

²³⁰ NSA October 2011 Minimization Procedures, *supra*, § 3(b)(5)(a).

²³¹ NSA October 2011 Minimization Procedures, *supra*, § 3(b)(5)(a)(1).

²³² NSA October 2011 Minimization Procedures, *supra*, § 3(b)(5)(a)(1)(a).

²³³ NSA October 2011 Minimization Procedures, *supra*, § 3(b)(5)(a)(1)(a).

²³⁴ Bates October 2011 Opinion, *supra*, at 18 n.17, 2011 WL 10945618, at *6 n.17.

²³⁵ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 4 n.2.

²³⁶ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 4 n.2.

information, however, may only be disseminated for law enforcement purposes,²³⁷ and the NCTC is not a law enforcement agency.²³⁸ The NCTC Section 702 minimization procedures require NCTC personnel who have been granted access to these FBI systems to first be trained to not use, retain, or disseminate purely law enforcement information, and to purge any such Section 702-acquired information from NCTC systems if it has been ingested.²³⁹

C. Querying the Acquired Data

The NSA, CIA, and FBI's Section 702 minimization procedures all permit these agencies to query unminimized Section 702-acquired information. A "query" refers to any instance where data is searched using a specific term or terms for the purpose of discovering or retrieving unminimized Section 702-acquired content or metadata. A query "term" or "identifier" is just like a search term that is used in an Internet search engine — the term could be, for example, an email address, a telephone number, a key word or phrase, or a specific identifier that an agency has assigned to an acquired communication.²⁴⁰ Queries are conducted using one or more of such terms or identifiers. Section 702 queries are of data that has already been acquired through the tasking of selectors as described above. A query therefore does not cause the government to collect any new communications, but queries do permit the government to more efficiently search through and discover information in the data the government has already acquired.²⁴¹

An aspect common to the implementation of the query provisions in all of the Section 702 minimization procedures is that an analyst or agent only receives unminimized Section 702-acquired data as a result of a query if that analyst or agent has the appropriate training and authorization to access the Section 702 data. Different agencies accomplish this in different ways. For example, the CIA limits access to the database containing unminimized Section 702-acquired data to personnel who have received training in the CIA's Section 702 minimization procedures, thereby preventing untrained individuals from conducting queries of this data. The NSA, on the other hand, often stores data acquired from multiple legal authorities in a single data repository. Instead of limiting access to whole databases, the NSA tags each acquired communication with the legal authority under which it was acquired, and then has systems that prevent an analyst from accessing or querying data acquired under a legal authority for which the analyst does not have the

²³⁷ 50 U.S.C. § 1801(h)(3).

²³⁸ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 4 n.2.

²³⁹ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 4 n.2.

²⁴⁰ *See, e.g.*, NSA DCLPO REPORT, *supra*, at 6; NSA October 2011 Minimization Procedures, *supra*, § 3(b)(6).

²⁴¹ PCLOB March 2014 Hearing Transcript, *supra*, at 29-31 (statements of Rajesh De, General Counsel, NSA and Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ).

requisite training.²⁴² At the FBI, an agent or analyst who conducts a “federated query” across multiple databases, but who does not have Section 702 training, would not receive the Section 702–acquired information as the result of a query. The agent or analyst would, however, be notified in their query results of the fact that there is responsive information to their query in a database containing unminimized Section 702–acquired information to which he or she does not have access. In order to gain access to this information, the analyst or agent would need to either take the requisite training to gain access to the Section 702 information or contact a fellow agent or analyst who had the requisite training to determine whether the responsive results can be disseminated pursuant to the minimization procedures.

The NSA’s intelligence analysts conduct at times complex queries across large data sets. The NSA’s minimization procedures require that queries of unminimized Section 702–acquired information be designed such that they are “reasonably likely to return foreign intelligence information.”²⁴³ This prohibition against overbroad queries (such as a query for the term “river” across all Section 702–acquired data with no other limiting query terms) or queries conducted for purposes other than to identify foreign intelligence information (such as an analyst’s query to find information about a girlfriend) applies to all of the NSA queries of unminimized Section 702–acquired information, not just queries containing U.S. person identifiers.²⁴⁴ NSA analysts receive training regarding how to use multiple query terms or other query discriminators (like a date range) to limit the information that is returned in response to their queries of the unminimized data.²⁴⁵ Through various means, the NSA systems record all queries of unminimized Section 702–acquired data, and these records are subject to audit.²⁴⁶

Additional rules apply when an NSA analyst wants to use a U.S. person identifier — i.e., a query term associated with a specific U.S. person, such as an email address or telephone number — to query unminimized Section 702–acquired data. U.S. person identifiers are prohibited from being used to query the NSA’s Section 702 upstream collection of Internet transactions.²⁴⁷ In contrast, the NSA’s upstream telephony collection

²⁴² See NSA DCLPO REPORT, *supra*, at 6-7.

²⁴³ NSA October 2011 Minimization Procedures, *supra*, § 3(b)(6).

²⁴⁴ See NSA DCLPO REPORT, *supra*, at 6-7 (discussing general query restrictions prior to detailing the additional requirements with regard to U.S. person identifiers).

²⁴⁵ NSA DCLPO REPORT, *supra*, at 6-7; see also NSA October 2011 Minimization Procedures, *supra*, § 3(b)(6) (noting that “other discriminators” may be used in constructing queries).

²⁴⁶ NSA DCLPO REPORT, *supra*, at 7.

²⁴⁷ NSA October 2011 Minimization Procedures, *supra*, § 3(b)(6).

and PRISM data may be queried using U.S. person identifiers if those U.S. person identifiers have been approved pursuant to internal NSA procedures.²⁴⁸

The NSA's internal procedures treat queries of metadata and content using U.S. person identifiers differently.²⁴⁹ The NSA's internal procedures require that queries of metadata using a U.S. person identifier be conducted only in a system or systems that require analysts to document the basis for their metadata query prior to conducting the query. Analysts are trained prior to using such systems. The NSA reported that it conducted approximately 9,500 metadata queries using U.S. person identifiers in 2013. In reviewing these queries, the NSD and ODNI have found that this number is likely substantially overinclusive of the actual number of U.S. person metadata queries conducted because many query terms that had been labeled as U.S. person identifiers proved on further analysis to not be identifiers of U.S. persons.

With respect to content queries using U.S. person identifiers, the NSA's internal procedures take a white-listing approach. Specifically, content queries using U.S. person identifiers are not permitted unless the U.S. person identifiers have been pre-approved (i.e., added to a white list) through one of several processes, several of which incorporate other FISA processes. For example, the NSA has approved the use of content queries using identifiers of U.S. persons currently subject to FISC-approved electronic surveillance under Section 105 or targeting under Section 704. U.S. person identifiers can also be approved by NSA's Office of General Counsel after a showing is made regarding why the proposed use of the U.S. person identifier would be "reasonably likely to return foreign intelligence information;" all approvals to use U.S. person identifiers to query content must be documented.²⁵⁰ In 2013, the NSA approved 198 U.S. person identifiers to be used as content query terms. The NSA minimization procedures mandate that the DOJ's National Security Division and ODNI conduct oversight of the NSA's U.S. person queries. The NSD and ODNI's oversight of the NSA and other agencies queries is further detailed below.

The CIA's minimization procedures similarly permit the CIA to query unminimized Section 702-acquired data using U.S. person identifiers to discover foreign intelligence information.²⁵¹ The CIA's minimization procedures require that all queries of unminimized content, whether or not a U.S. person identifier is used in the query, must be "reasonably designed to find and extract foreign intelligence information." The CIA minimization procedures state that the CIA must keep records of all such content queries.

²⁴⁸ NSA October 2011 Minimization Procedures, *supra*, § 3(b)(6).

²⁴⁹ NSA DCLPO REPORT, *supra*, at 7.

²⁵⁰ NSA October 2011 Minimization Procedures, *supra*, § 3(b)(6); NSA DCLPO REPORT, *supra*, at 7.

²⁵¹ Bates October 2011 Opinion, *supra*, at 25, 2011 WL 10945618, at *8; AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 13.

In implementing its query provision, the CIA has not required its personnel to seek pre-approval of U.S. person content queries, but it does record who conducts those queries and requires analysts to both identify any U.S. person identifiers used as query terms and to write a contemporaneous foreign intelligence justification for any query of unminimized Section 702-acquired content using a U.S. person identifier.²⁵² The CIA's content queries, for example, involve U.S. persons located overseas that intelligence indicates may be engaged in facilitating international terrorism.

In 2013, the CIA conducted approximately 1,900 content queries using U.S. person identifiers. Approximately forty percent of these content queries were at the request of other U.S. intelligence agencies. Some identifiers were queried more than once; the CIA has advised that approximately 1,400 unique identifiers were queried during this period. The NSD and ODNI are required under the CIA minimization procedures to review these records.

Metadata queries are treated differently under the CIA's minimization procedures. The CIA minimization procedures do not contain a standard for conducting metadata queries, although the statute and internal CIA procedures do require that queries may not be conducted for an unauthorized purpose (such as trying to find information about a love interest). If the CIA did identify any metadata associated with the individual, however, the CIA is permitted to conduct a further query into the underlying content only if the query is to identify foreign intelligence information, and the CIA may only disseminate the results of content or metadata queries to the requesting entity if the dissemination of information was otherwise permissible under the CIA's minimization procedures, as described below. The CIA does not track how many metadata-only queries using U.S. person identities have been conducted.

The FBI minimization procedures also permit the FBI to query unminimized Section 702-acquired data.²⁵³ Stemming from its role as both a foreign intelligence and a law enforcement agency, the FBI's minimization procedures differ from the NSA and CIA's procedures insofar as they permit the FBI to conduct reasonably designed queries "to find and extract" both "foreign intelligence information" and "evidence of a crime." Although, consistent with 50 U.S.C. § 1806(a), any use of Section 702-acquired information regarding United States or non-U.S. persons may only be used for lawful purposes, the requirement that queries be reasonably designed to identify foreign intelligence information or evidence

²⁵² AUGUST 2013 SEMI-ANNUAL ASSESSMENT, *supra*, at 8 ("NSD and ODNI also review CIA's written justifications for all queries using United States person identifiers of the content of unminimized Section 702-acquired communications.").

²⁵³ PCLOB March 2014 Hearing Transcript, *supra*, at 86 (statement of James A. Baker, General Counsel, FBI) (noting that the FBI queries such data).

of a crime applies only to U.S. person information. The “reasonably designed” standard applies to both content and metadata queries.

The FBI is required under its minimization procedures to maintain records of all terms used to query content. These records identify the agent or analyst who conducted the query, but do not identify whether the query terms are U.S. person identifiers. Although the FBI's minimization procedures do not require the FBI to keep records of metadata-only queries, such queries are conducted in the same databases that contain the content collection; therefore, such metadata queries are also recorded. The NSD and ODNI conduct oversight reviews of both the content and metadata queries, as described below.

Because they are not identified as such in FBI systems, the FBI does not track the number of queries using U.S. person identifiers. The number of such queries, however, is substantial for two reasons.

First, the FBI stores electronic data obtained from traditional FISA electronic surveillance and physical searches, which often target U.S. persons, in the same repositories as the FBI stores Section 702–acquired data, which cannot be acquired through the intentional targeting of U.S. persons. As such, FBI agents and analysts who query data using the identifiers of their U.S. person traditional FISA targets will also simultaneously query Section 702–acquired data.

Second, whenever the FBI opens a new national security investigation or assessment, FBI personnel will query previously acquired information from a variety of sources, including Section 702, for information relevant to the investigation or assessment. With some frequency, FBI personnel will also query this data, including Section 702–acquired information, in the course of criminal investigations and assessments that are unrelated to national security efforts. In the case of an assessment, an assessment may be initiated “to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security or to collect foreign intelligence information.”²⁵⁴ If the agent or analyst conducting these queries has had the training required for access to unminimized Section 702–acquired data, any results from the Section 702 data would be returned in these queries. If an agent or analyst does not have access to unminimized Section 702–acquired data — typically because this agent or analyst is assigned to non-national security criminal matters only — the agent or analyst would not be able to view the unminimized data, but would be notified that data responsive to the query exists and could request that an agent or analyst with the proper training and access to review the unminimized Section 702–acquired data. Anecdotally, the FBI has advised the Board that it

²⁵⁴ The Attorney General’s Guidelines for Domestic FBI Operations § II.A, *available at* <http://www.justice.gov/ag/readingroom/guidelines.pdf>.

is extremely unlikely that an agent or analyst who is conducting an assessment of a non-national security crime would get a responsive result from the query against the Section 702-acquired data.

D. Retention and Purging

FISA also requires that the retention of nonpublicly available U.S. person information be minimized consistent with the need of the United States to obtain, produce, and disseminate information.²⁵⁵ As such, the NSA, CIA, and FBI's minimization procedures contain provisions regarding when unminimized data must be aged off agency systems, what data must be purged upon recognition, and what types of evaluated information may be retained indefinitely.²⁵⁶ Data that has been evaluated and determined to contain either no U.S. person information or only U.S. person information that meets the standard for permanent retention is referred to as "minimized information."

With a notable exception, unminimized Section 702-acquired data must be aged off of the NSA and CIA systems no later than five years after the expiration of the Section 702 certification under which that data was acquired.²⁵⁷ Unminimized Internet transactions acquired through the NSA's upstream collection, however, must be aged off of the NSA systems no later than two years after the expiration of the Section 702 certification under which the data has been acquired.²⁵⁸ The CIA and FBI do not receive, and therefore do not retain, such upstream collection. The FBI's minimization procedures alone distinguish between acquired data that have not been reviewed and those that have not been determined to meet the retention standard. As with the NSA and CIA, Section 702-acquired communications that have not been reviewed must be aged off FBI systems no later than five years after the expiration of the Section 702 certifications under which the data was acquired. Data that was reviewed but not yet determined to meet the retention standard in the FBI minimization procedures may be kept for a longer retention period subject to additional access controls.

With respect to all of the agencies, extensions from these age-off requirements may be sought from a high-level agency official. Other limited exceptions apply, such as to communications that are still being decrypted.²⁵⁹

²⁵⁵ 50 U.S.C. § 1801(h)(1).

²⁵⁶ Although the minimization procedures themselves do not place an outer limit regarding how long such information may be retained, general rules regarding the retention of federal records apply to this data.

²⁵⁷ See, e.g., NSA October 2011 Minimization Procedures, *supra*, § 3(c)(1); NSA DCLPO REPORT, *supra*, at 8.

²⁵⁸ NSA October 2011 Minimization Procedures, *supra*, § 3(c)(1); NSA DCLPO REPORT, *supra*, at 8.

²⁵⁹ See, e.g., NSA October 2011 Minimization Procedures, *supra*, § 6(a)(1)(a).

As government personnel engage in the process of evaluating communications, the minimization procedures impose certain requirements requiring communications to be purged upon recognition. As described above, if data has been acquired as a result of a compliance incident, such as a typographical error in the tasking or a failure to detask a selector before a target's known travel to the United States, any identifiable data acquired as a result of the compliance incident is purged.²⁶⁰ When a compliance incident is discovered, each agency has a process to discover and destroy data subject to purge.²⁶¹ The agencies also must coordinate such purges to ensure that all agencies are both aware of instances when a purge is required and use the same parameters to identify data subject to purge.²⁶²

Whether or not the communications were acquired as a result of a compliance incident, purges are required whenever a user of a tasked selector has been determined to be a U.S. person or located in the United States at any point during the acquisition.²⁶³ These purge requirements, and the exceptions to these requirements, have been detailed above. In addition, the NSA's minimization procedures include additional purge-upon-recognition requirements due to the possibility that the NSA's upstream collection of Internet transactions could acquire domestic communications to which a user of a tasked selector is not a communicant. Such upstream-acquired Internet transactions must be destroyed upon recognition if it is determined that the transactions contain U.S. person information but do not contain any information that meets the NSA's long-term retention standards (discussed further below).²⁶⁴ MCTs must also be destroyed upon recognition if it is determined that a single, discrete communication within the MCT is a wholly domestic communication.²⁶⁵

The NSA's minimization procedures also contain the following provision:

Personnel will exercise reasonable judgment in determining whether information acquired must be minimized and will destroy inadvertently

²⁶⁰ See, e.g., PCLOB March 2014 Hearing Transcript, *supra*, at 72.

²⁶¹ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-13.

²⁶² AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-13.

²⁶³ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-12 (noting that all of the agency minimization procedures require purges when a target is discovered to be a U.S. person or person located in the United States, with limited exceptions).

²⁶⁴ NSA October 2011 Minimization Procedures, *supra*, § 3(c)(2).

²⁶⁵ NSA October 2011 Minimization Procedures, *supra*, § 3(b)(5)(a)(1)(a) (requiring destruction of segregated MCTs determined to contain a wholly domestic communication) and § 3(b)(5)(b)(1) (requiring a determination regarding whether a single communication within an MCT is a wholly domestic communication before it is used); Bates November 2011 Opinion, *supra*, at 9, 2011 WL 10947772, at *4 (incorporating government's representation in a filing that if the discrete communication within an MCT is determined to be a wholly domestic communication, it must be destroyed).

acquired communications of or concerning a United States person at the earliest practicable point in the processing cycle 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.²⁶⁶

While it is not entirely clear what constitutes an “inadvertently acquired communication” here, the NSA’s general counsel has stated that “[i]f information is determined to not have foreign intelligence value then it is required to be purged.”²⁶⁷ The NSA’s general counsel, however, clarified that it is often “difficult to determine the foreign intelligence value of any particular piece of information.”²⁶⁸ An NSA analyst would need to determine not only that a communication is not currently of foreign intelligence value to him or her, but also would not be of foreign intelligence value to any other present or future foreign intelligence need. Thus, in practice, this requirement rarely results in actual purging of data.

Neither the CIA nor FBI’s minimization procedures have comparable requirements that a communication containing U.S. person information be purged upon recognition that the communication contains no foreign intelligence information; instead the CIA and FBI rely solely upon the overall age-off requirements found in their minimization procedures.

Section 702–acquired data that is not subject to purge upon recognition may be retained effectively indefinitely (i.e., need not be aged off of agency systems) if an agency determines that the data meets the retention standard in its minimization procedures. A communication is sometimes described as having been “minimized” or “retained” if the communication has been determined to meet this retention standard.

The NSA’s minimization procedures permit the NSA to retain communications (other than wholly domestic communications) in generally the same situations where the NSA is permitted to disseminate (i.e., disclose) these communications to the consumers of the NSA’s intelligence reports.²⁶⁹ Specifically, the NSA may retain communications where the information identifiable to a U.S. person is, for example, “necessary to understand the foreign intelligence information or assess its importance,” indicates that U.S. person “may be the target of intelligence activities” by a foreign government, or “the communication indicates that the United States person may be engaging international terrorist

²⁶⁶ NSA October 2011 Minimization Procedures, *supra*, § 3(b)(1).

²⁶⁷ PCLOB March 2014 Hearing Transcript, *supra*, at 44; *see also id.* at 45-46 (referencing above quoted provision in the minimization procedures by stating that this determination must be made “as early as possible in . . . the processing cycle”).

²⁶⁸ PCLOB March 2014 Hearing Transcript, *supra*, at 46.

²⁶⁹ NSA October 2011 Minimization Procedures, *supra*, § 6(a).

activities.”²⁷⁰ The NSA may also retain a communication containing U.S. person information if the communication is reasonably believed to contain evidence of a crime and the NSA has or will disseminate that evidence to a federal law enforcement entity.²⁷¹ The NSA may also retain communications beyond the normal age-off period if it is still decrypting the communication or using the communication to decrypt other communications.²⁷²

The NSA minimization procedures do not separately place any limitations on the retention of communications that contain no U.S. person information, but they do contain a reminder that any such communications may be retained only in accordance with other laws, regulations, and policy (for example, the general definitions and restrictions regarding the NSA’s authorities provided in Executive Order 12333 and related documents).²⁷³

The retention standard in the CIA’s Section 702 minimization procedures is comparable to the standard found in the NSA’s minimization procedures. The CIA may indefinitely retain “minimized” communications. In order to “minimize” the communication, the CIA must remove any U.S. person information from the communication unless the information is publicly available, the U.S. person has consented to retention of the information, or the CIA must determine that the U.S. person information is necessary or may reasonably become necessary to understand foreign intelligence information. The CIA minimization procedures contain various categories of information considered to either be foreign intelligence information or information that is necessary to understand foreign intelligence information. Once “minimized,” the communications may be retained in repositories that are still restricted to CIA personnel, but not necessarily CIA personnel who have been trained in the CIA minimization procedures. The CIA minimization procedures also permit the retention of data that is retained because it has been reported to a federal law enforcement agency as evidence of a crime.

The FBI Section 702 minimization procedures permit acquired communications to be retained indefinitely if the communications either contain no U.S. person information or if the communications contain information that “reasonably appears to be foreign intelligence information, [is] necessary to understand foreign intelligence information or assess its importance, or [is] evidence of a crime.” Before further using this communication, the FBI is required to “mask” any U.S. person information within the communication that does not satisfy one of these three criteria. The FBI is also separately required to retain

²⁷⁰ NSA October 2011 Minimization Procedures, *supra*, § 6(a)(2), (b).

²⁷¹ NSA October 2011 Minimization Procedures, *supra*, § 6(a)(3), (b)(8).

²⁷² NSA October 2011 Minimization Procedures, *supra*, § 6(a)(1).

²⁷³ NSA October 2011 Minimization Procedures, *supra*, § 7.

reviewed information that reasonably appears to be exculpatory or that reasonably appears to be discoverable in a criminal proceeding.

E. Use and Dissemination

Restrictions in FISA and the minimization procedures contain limitations on the use and dissemination of Section 702–acquired information. “Dissemination” of FISA-acquired information generally refers to the reporting of acquired information outside of an intelligence agency, though broad accessibility of information within an agency can also constitute dissemination.²⁷⁴

Section 702 acquisition is governed by almost all of the same restrictions on use that apply to traditional FISA electronic surveillance.²⁷⁵ These statutory restrictions apply to both U.S. person information and non-U.S. person information. Specifically, all Section 702 information may be used or disclosed only for lawful purposes.²⁷⁶ Use of Section 702–acquired information in a criminal proceeding must be authorized by the Attorney General.²⁷⁷ Any person whose communications have been acquired pursuant to Section 702, whether or not he or she was a target of the acquisition and whether or not he or she is a U.S. person, must be notified by the government before any information obtained from or derived from Section 702 acquisition is used against him or her in any legal proceeding in the United States.²⁷⁸ Such an individual is referred to as an “aggrieved person.” An aggrieved person may move to suppress the evidence that was obtained from or derived from Section 702 acquisition on the grounds that the information was unlawfully acquired or that the Section 702 acquisition otherwise did not conform with the Attorney General and Director of National Intelligence’s authorization.²⁷⁹

The agencies’ minimization procedures and practices impose additional restrictions on the use and dissemination of Section 702–acquired data. The NSA’s minimization procedures permit the NSA to disseminate U.S. person information if the NSA deletes any information that could identify the U.S. person (a process referred to as “masking”).²⁸⁰ Alternatively, the NSA may disseminate the U.S. person’s identity for one of a specific list of reasons, including that the U.S. person has consented to the dissemination, the specific

²⁷⁴ See H.R. Rep. No. 95-1283, at 59 (discussing minimization within agencies).

²⁷⁵ 50 U.S.C. § 1881e(a) (stating that information acquired under Section 702 shall be governed under virtually all of the use restrictions found in 50 U.S.C. § 1806).

²⁷⁶ 50 U.S.C. § 1806(a).

²⁷⁷ 50 U.S.C. § 1806(b).

²⁷⁸ 50 U.S.C. § 1806(c), (d).

²⁷⁹ 50 U.S.C. § 1806(e).

²⁸⁰ NSA October 2011 Minimization Procedures, *supra*, § 6 (b).

information about the U.S. person is already publicly available, the U.S. person's identity is necessary to understand foreign intelligence information, or the communication contains evidence of a crime and is being disseminated to law enforcement authorities. As a matter of practice and policy, the NSA typically masks all information that could identify a U.S. person in its reports.²⁸¹ Consumers of NSA reports, such as other federal agencies, may then request that the U.S. person identity be "unmasked," a request that the NSA approves if the user has a "need to know" and disseminating the U.S. person identity would be consistent with the NSA's minimization procedures.²⁸²

Generally, dissemination of communications that contain no U.S. person information are governed by other laws, regulation, and policies (such as Executive Order 12333 and related implementing regulations), but not by the minimization procedures.²⁸³ These further restrictions outside the minimization procedures, for example, require that the NSA generate intelligence reports only to meet specific intelligence requirements established by the government.²⁸⁴ These regulations and policies also contain restrictions regarding what information (U.S. person information or otherwise) may be shared with foreign governments.²⁸⁵

In response to Judge Bates' opinion finding that a previous version of the NSA's minimization procedures did not meet Fourth Amendment or statutory requirements, the NSA's minimization procedures now also impose additional restrictions on the use of MCTs. Specifically, before a discrete communication contained within an MCT can be used in an intelligence report, FISA application, or to engage in further Section 702 targeting, the NSA analyst must determine if the discrete communication contains a tasked selector.²⁸⁶ If not, and the communication is to or from an identifiable U.S. person or person located in the United States, that discrete communication may only be used to protect against an immediate threat to life, such as a hostage situation.²⁸⁷

The CIA's minimization procedures permit the CIA to disseminate U.S. person information if any information that identifies the U.S. person is masked in the dissemination. The CIA may also disseminate U.S. person information in a manner that identifies the U.S. person if that person's identity is necessary to understand foreign

²⁸¹ NSA DCLPO REPORT, *supra*, at 7.

²⁸² NSA DCLPO REPORT, *supra*, at 7-8; NSA October 2011 Minimization Procedures, *supra*, §§ 6(b) and 7.

²⁸³ NSA October 2011 Minimization Procedures, *supra*, § 7.

²⁸⁴ NSA DCLPO REPORT, *supra*, at 7.

²⁸⁵ *See generally* Exec. Order No. 12333 §§ 1.3(b)(4) and 1.6(f).

²⁸⁶ NSA October 2011 Minimization Procedures, *supra*, § 3(b)(5)(b)(2).

²⁸⁷ NSA October 2011 Minimization Procedures, *supra*, § 3(b)(5)(b)(2)(c).

intelligence information or (if concerning an attack by a foreign power, sabotage by a foreign power, international terrorism or the international proliferation of weapon of mass destruction by a foreign power, or clandestine intelligence activities by a foreign power) may become necessary to understand the foreign intelligence information. The CIA may further disseminate evidence of a crime to federal law enforcement authorities.

The FBI's minimization procedures permit the FBI to disseminate Section 702-acquired U.S. person information that reasonably appears to be foreign intelligence information or is necessary to understand foreign intelligence information. Disseminations concerning the national defense or security of the United States or the conduct of foreign affairs of the United States are permitted to identify U.S. persons only if necessary to understand the foreign intelligence information or to assess its importance. The FBI is also permitted to disseminate U.S. person information that reasonably appears to be evidence of a crime to law enforcement authorities. The FBI's minimization procedures incorporate certain guidelines, already otherwise applicable to the FBI, regarding the dissemination of information to foreign governments.²⁸⁸

VII. Internal Agency Oversight and Management of the Section 702 Program

In addition to the training programs previously described, each of the agencies subject to targeting or minimization procedures has developed a corresponding compliance program to evaluate and oversee compliance with these procedures, as well as facilitate the reviews by external overseers.²⁸⁹ Any incidents of noncompliance that have been identified either by these compliance programs or that are otherwise discovered by the agencies must be reported to the DOJ and ODNI, who in turn must report these incidents to Congress and the FISC,²⁹⁰ as discussed in the next section.

The NSA's use of the Section 702 authorities are internally overseen by various NSA entities, including the NSA's Office of the Director of Compliance ("ODOC"), NSA's Office of General Counsel ("OGC"), embedded compliance elements within NSA's directorates (in

²⁸⁸ NSA October 2011 Minimization Procedures, *supra*, § 3(b)(5)(b)(2)(c).

²⁸⁹ See AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-6 to A-8 (discussing NSA oversight program); *id.* at A-9 (discussing CIA oversight program); *id.* at A-11 to A-12 (discussing FBI oversight program). See *generally id.* at 4-5 n.2 (noting that no incidents of noncompliance have been reported by the NCTC and that the NSD and ODNI would be conducting a review of the NCTC's compliance in the following reporting period).

²⁹⁰ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 28 (noting that the semiannual report required by Section 707 is given to both Congress and the FISC and describes all incidents of noncompliance); 50 U.S.C. § 1881f(b)(1)(G) (requiring all incidents of noncompliance with the targeting procedures, minimization procedures, and Attorney General Guidelines, as well as any incidents of noncompliance by a provider, to be reported in the Section 707 Report); FISC Rule of Procedure 13(b) (requiring incidents of noncompliance to be reported to the FISC).

particular, the Signals Intelligence Directorate's Oversight and Compliance ("O&C" section), and — as of early 2014 — the NSA's new Director of Civil Liberties and Privacy Office ("DCLPO").²⁹¹ Each of these organizations has different, but related, roles. The NSA's ODOC is responsible for NSA-wide compliance efforts and conducts periodic risk assessments to identify potential systemic incidents of noncompliance with the NSA targeting or minimization procedures.²⁹² For example, the ODOC conducted a risk assessment regarding how effective the NSA's purge practices had been in removing data required to be purged from the NSA's systems. Particularly important in light of errors and misunderstandings that have led to compliance issues in Section 702 and other programs, such as the MCT issue discussed above, ODOC also coordinates programs intended to ensure that factual representations made to the FISC are accurate and that interpretations of how the targeting and minimization procedures are to be applied in practice are consistent both within the NSA and between the NSA and its overseers.²⁹³

The NSA's O&C section and OGC conduct more granular oversight of the Section 702 program. The O&C section conducts spot checks of individual targeting decisions, queries of acquired data, and disseminations for compliance with the NSA's targeting and minimization procedures.²⁹⁴ The O&C section and OGC also offer compliance-related guidance regarding targeting decisions, investigate and report potential incidents of noncompliance with the procedures and other legal requirements, and provide remedial training when an incident investigation reveals that the incident was caused by an avoidable error.²⁹⁵ The O&C section and OGC also facilitate the reviews conducted by the DOJ and ODNI that are described below.²⁹⁶

The NSA appointed its first Director of Civil Liberties and Privacy while the Board was conducting its review of the Section 702 program. The Director's office is not, as of yet, involved in periodic Section 702 programmatic reviews. The Director's first public report, however, was issued in April 2014 and described in an unclassified manner aspects of the NSA's implementation of the Section 702 program.

The CIA's internal compliance program is managed by the CIA's FISA Program Office and the CIA's OGC.²⁹⁷ These entities conduct oversight of the CIA's day-to-day use of the Section 702 authorities by, for example, conducting pre-tasking reviews of the CIA

²⁹¹ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-6 to A-8; NSA DCLPO REPORT, *supra*, at 9.

²⁹² AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-7 to A-8.

²⁹³ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-7.

²⁹⁴ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-7; NSA DCLPO REPORT, *supra*, at 7.

²⁹⁵ *See generally* NSA DCLPO REPORT, *supra*, at 9.

²⁹⁶ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 7.

²⁹⁷ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-9.

nominations to the NSA regarding proposed new selectors to be tasked for Section 702 acquisition.²⁹⁸ The FISA Program Office also oversees whether current and proposed systems handle Section 702-acquired data in compliance with the minimization procedures.²⁹⁹ The FISA Program Office additionally conducts reviews regarding whether Section 702 selectors remain properly tasked.³⁰⁰ The CIA's OGC has attorneys embedded with CIA personnel to answer specific targeting, querying, retention, and dissemination questions.³⁰¹ Finally, the CIA FISA program office and the CIA OGC facilitate the reviews conducted by the DOJ and ODNI that are described below.

Several sub-organizations within the FBI are responsible for conducting internal oversight over the Bureau's Section 702 activities. The FBI's OGC, in particular its National Security Law Branch, is responsible for providing legal advice regarding the application of the FBI targeting and minimization procedures. The FBI's Exploitation Threat Section ("XTS") takes the lead in reviewing the FBI's nominations to the NSA for proposed Section 702 tasking.³⁰² Various sub-organizations within the Bureau are responsible for reviewing and monitoring compliance with the FBI targeting and minimization procedures.

As described above, the NCTC's role in the Section 702 program is minimal. The NCTC has assigned legal and program personnel to oversee the implementation of its minimization procedures.

Incidents of noncompliance with the targeting or minimization procedures that are identified by any of these internal compliance efforts, or that are otherwise self-identified by the agencies, must be reported to the DOJ and ODNI.³⁰³ Historically, most identified compliance incidents have been discovered as a result of self-reporting or via the internal compliance programs.³⁰⁴ Once an incident has been identified and reported, the internal

²⁹⁸ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-8 to A-9.

²⁹⁹ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-9.

³⁰⁰ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-9.

³⁰¹ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-9.

³⁰² AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-12.

³⁰³ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 7 (regarding the NSA's reporting of incidents), 10 (regarding reporting of incidents by the FBI Office of General Counsel), A-7 (regarding the NSA's reporting via the NSA Office of General Counsel), and A-9 (regarding reporting of incidents by the CIA Office of General Counsel).

³⁰⁴ See AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 7 (stating that most incidents "are identified by NSA analysts or by NSA's internal compliance program"); *id.* at 25 (noting that most compliance incidents involve the NSA targeting or minimization procedures); *id.* at 28 (advising that the "volume" of NSA incidents is robust enough such that pattern and trend analysis is more fruitful than is the case with other compliance matters).

compliance programs are also involved in implementing remedial actions, such as purging and retraining as required.³⁰⁵

In addition to reporting incidents of noncompliance, as an additional prophylactic measure the NSA is required under its targeting procedures to report any instance in which a user of a Section 702–tasked selector is determined to have been in the United States while the selector was tasked.³⁰⁶ Should the CIA or FBI determine that a user of a Section 702 selector is a U.S. person or located in the United States, the CIA and FBI report this to the NSA, which in addition to promptly detasking the selector, sends a report to the DOJ and ODNI. This reporting requirement applies whether or not the NSA assesses that this acquisition occurred as the result of a compliance incident. For example, if the NSA correctly assessed that a target was a non-U.S. person located abroad, but unbeknownst to the NSA (and not reasonably predictable based on information available to the NSA), the target subsequently entered the United States, no compliance incident would have occurred. The NSA would be required to promptly detask the target’s selectors from Section 702 acquisition upon recognition and purge data acquired while the user was in the United States, but no incident of noncompliance with the targeting or minimization procedures would have occurred. This is because the NSA assessed that the target was a non-U.S. person reasonably believed to be located outside the United States up until the time that the NSA detasked the selector from Section 702 acquisition. Nonetheless, the NSA would be required to report such an incident to the DOJ and ODNI. As described below, the DOJ and ODNI investigate such incidents and will request additional information in order to make their own determination regarding whether a compliance incident did or did not occur.³⁰⁷

Additionally, but separately, the statute also requires each agency that conducts Section 702 acquisition to conduct an annual review of the Section 702 program.³⁰⁸ These annual reviews must be sent to the Senate Select Committee on Intelligence, Senate Committee on the Judiciary, House Permanent Select Committee on Intelligence, and House Judiciary Committee (hereinafter, “the Congressional Committees”), the FISC, Attorney General, and Director of National Intelligence.³⁰⁹ The annual reviews must report the number of disseminations of U.S. person identities made, the number of U.S. person identities that were subsequently unmasked, and the number of Section 702 targets that

³⁰⁵ See, e.g., NSA DCLPO REPORT, *supra*, at 9 (regarding various remedies implemented by NSA after an incident is discovered); AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-13 (describing elements of the purge process).

³⁰⁶ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 7.

³⁰⁷ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 7.

³⁰⁸ 50 U.S.C. § 1881a(l)(3).

³⁰⁹ 50 U.S.C. § 1881a(l)(3).

were subsequently determined to be located in the United States.³¹⁰ The agency reviews must also evaluate whether foreign intelligence information is being acquired under the Section 702 program and whether the minimization procedures adequately minimize the acquisition, retention, and dissemination of U.S. person information consistent with the United States' foreign intelligence needs.³¹¹ The CIA receives Section 702 acquisition but does not actually conduct any acquisition. As such, the CIA does not conduct an annual review; some information regarding the CIA's use of the program, however, is included in the NSA's annual report.

VIII. External Oversight of the Section 702 Program

In enacting Section 702, Congress mandated additional external layers of oversight, each resulting in reports made to Congress and the FISC. This Section describes the targeting and minimization reviews conducted by the DOJ's National Security Division ("NSD") and the ODNI, the reports issued by the inspectors general, and additional oversight activities conducted by the FISC and the Congressional Committees.

A. NSD/ODNI Targeting Reviews

As is discussed above, the NSA is required under its targeting procedures to document every targeting decision made under its targeting procedures. The record of each targeting decision, known as a tasking sheet, includes (1) the specific selector to be tasked,³¹² (2) citations to the specific documents and communications that led the NSA to determine that the target is reasonably believed to be located outside the United States,³¹³ (3) a narrative describing the contents of these specific documents and communications, (4) a statement regarding the assessed U.S. person status of the target, and (5) a statement identifying the foreign power or foreign territory regarding which the foreign intelligence information is to be acquired.³¹⁴

The NSD conducts a post-tasking review of every tasking sheet provided by the NSA;³¹⁵ the ODNI reviews a sample of these sheets. In addition to evaluating whether the tasking complied with the targeting procedures, the NSD and ODNI review the targeting for

³¹⁰ 50 U.S.C. § 1881a(l)(3)(A)(i)-(iii).

³¹¹ 50 U.S.C. § 1881a(l)(3)(A), (B).

³¹² AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 7.

³¹³ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-5; *see also* NSA DCLPO REPORT, *supra*, at 4-5.

³¹⁴ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-5.

³¹⁵ *See* PCLOB March 2014 Hearing Transcript, *supra*, at 61 (statement of Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ) (stating that tasking sheets "are all reviewed . . . by the Department of Justice on a regular basis").

overall compliance with the statutory limitations, such as the prohibition against reverse targeting. If the NSD or ODNI is unable to determine whether the tasking sheet is sufficient, the NSD and ODNI will require the NSA to provide the cited documents and communications that underlie the NSA's foreignness determination at a bimonthly onsite review.³¹⁶ The NSD and ODNI also engage with the NSA compliance and legal personnel to ask follow-up questions regarding the foreignness and foreign intelligence purpose determinations.³¹⁷ As needed, the NSD and ODNI also seek additional information from the CIA and FBI regarding selectors that they have nominated.³¹⁸ The NSD and ODNI's review of foreign intelligence purpose determinations is more limited than its review of foreignness determinations insofar as the NSA analysts are required to document the basis for their foreignness determination (i.e., they must show their work), whereas the analyst need only identify a foreign intelligence purpose. The results of each NSD/ODNI bimonthly review are required by statute to be provided to the Congressional Committees.³¹⁹ Historically, the NSD and ODNI's bimonthly reviews have determined that approximately 0.1% of all the NSA taskings did not meet the requirements of the NSA targeting procedures.³²⁰

Additionally but separately, the NSD and ODNI also conduct approximately monthly reviews of the FBI's application of its own targeting procedures.³²¹ The NSD currently reviews every instance in which the FBI's evaluation of foreignness revealed any information regarding the target, regardless of whether the information confirms or rebuts the NSA's foreignness determination. Follow-up questions regarding the FBI's evaluation of this information are discussed with FBI analysts and supervisory personnel.³²² Like the NSA reviews, the results of the NSD/ODNI monthly reviews regarding FBI targeting are documented in a report that must be sent to the Congressional Committees.³²³ The NSD and ODNI have not reported the historical percentage of tasking incidents that have been discovered as a result of these reviews. For the period of June through November 2012, the

³¹⁶ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 7.

³¹⁷ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 7.

³¹⁸ *See, e.g.*, AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 8 (noting that with respect to CIA nominations "the joint oversight review team conducts onsite visits at CIA" and "the results of these visits are included in the bimonthly NSA review reports discussed above"); *see also* AUGUST 2013 SEMIANNUAL ASSESSMENT, at 6-7 (describing these content of the bimonthly review reports, including the NSA tasking review).

³¹⁹ 50 U.S.C. § 1881f(b)(1)(F).

³²⁰ PCLOB March 2014 Hearing Transcript, *supra*, at 43 (statement of Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ).

³²¹ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 9-10.

³²² AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 10.

³²³ 50 U.S.C. § 1881f(b)(1)(F).

overall FBI tasking incident error rate, which would include incidents discovered by the NSD/ODNI reviews, was 0.04%.

B. NSD/ODNI Minimization Reviews

The NSD and ODNI also conduct at least bimonthly reviews of the NSA, CIA, and FBI's application of their respective minimization procedures.³²⁴ These reviews vary based on the differences in each agency's minimization procedures and the manner in which each agency uses the Section 702-acquired data.³²⁵ In addition to reviewing agency activities for compliance with the minimization procedures, the NSD and ODNI also look for any other potential violations of statutory prohibitions, such as the prohibition against reverse targeting. For example, if a Section 702 tasking resulted in substantial reporting by the Intelligence Community regarding a U.S. person, but little about the Section 702 target, this would be a strong indication to the oversight team that reverse targeting may have occurred. The results of the NSD/ODNI reviews are documented in reports that are, as required by FISA, sent to the Congressional Committees.³²⁶

The NSD and ODNI bimonthly minimization reviews at the NSA focus on dissemination and queries using U.S. person identifiers.³²⁷ With respect to dissemination, the NSA identifies to the NSD/ODNI review team all NSA-issued reports that contain U.S. person information derived from Section 702 acquisition.³²⁸ The NSD/ODNI team has reviewed a substantial majority of these reports.³²⁹ The NSD/ODNI team also reviews other disseminations of foreign intelligence information to foreign governments, which may or may not contain U.S. person information.³³⁰ With respect to queries of Section 702-acquired metadata using U.S. person identifiers, the NSD/ODNI team reviews all such queries and analysts' justifications for the queries. With respect to Section 702-acquired content queries, the NSD/ODNI review team reviews the documentation for all U.S. person identifiers that are approved as query terms.³³¹

³²⁴ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 5-10 (regarding frequency of reviews and fact that they include minimization reviews).

³²⁵ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 5-6.

³²⁶ 50 U.S.C. § 1881f(b)(1)(F).

³²⁷ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 7, 13.

³²⁸ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 7.

³²⁹ The NSD/ODNI previously reviewed a substantial majority of these reports. *See* NSA DCLPO REPORT, *supra*, at 8. NSD has advised that it has recently revised its reviews and is now reviewing all reports provided by NSA that that contain U.S. person information.

³³⁰ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 7.

³³¹ *See* NSA October 2011 Minimization Procedures, *supra*, § 3(b)(6) (regarding documentation requirements for such query terms); NSA DCLPO REPORT, *supra*, at 7 (regarding fact that this documentation is made available to NSD and ODNI for review).

At the CIA, the NSD/ODNI team reviews the CIA's querying, retention, and dissemination of Section 702-acquired data.³³² The NSD/ODNI team evaluates all of the required written justifications for use of a U.S. person identifier (or any other query term intended to return information about a particular U.S. person) to query Section 702-acquired content.³³³ Metadata queries are not reviewed. The NSD/ODNI review team samples decisions made by CIA personnel to permanently retain data.³³⁴ The CIA is required to provide, and the NSD/ODNI team reviews, all disseminations of Section 702-acquired U.S. person information.³³⁵

With respect to the FBI, the NSD/ODNI team also evaluates the FBI's querying, retention, and dissemination determinations.³³⁶ The NSD and ODNI review a sample of communications that FBI assesses meets the retention standards, a sample of disseminations containing Section 702-derived U.S. person information, and a sample of queries conducted by FBI personnel.

The NSD and ODNI also conduct annual process reviews at the NCTC and FBI. The NCTC process review examines the processes that the NCTC has put in place to control access and train personnel with regard to its limited Section 702 minimization procedures. The FBI annual process review surveys the systems FBI uses to receive, verify, and route PRISM collection.

The NSD and ODNI also conduct ad hoc reviews related to newly developed or modified systems that the agencies plan to use to target non-U.S. persons under Section 702 or acquire, retain, or disseminate Section 702-acquired information.³³⁷ These ad hoc system reviews are intended to identify existing compliance issues, prevent future compliance incidents from occurring, and ensure that systems are designed in a manner that facilitates subsequent oversight of their use.

C. NSD/ODNI Incident Investigation, Reporting, and Related Activities

Whether initially discovered via an NSD/ODNI review, an internal agency compliance review, or by self-reporting, Section 702 and the FISC's own rules of procedure require the NSD to report compliance incidents by the Intelligence Community or electronic communication service providers to the Congressional Committees and to the

³³² AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 8.

³³³ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 8.

³³⁴ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 8.

³³⁵ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 8.

³³⁶ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 10 & n.6.

³³⁷ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 11.

FISC.³³⁸ Specifically, the FISA Amendments Act requires the Attorney General to report every incident of noncompliance to the Congressional Committees in a semiannual report.³³⁹ Pursuant to FISC Rule of Procedure 13(b), all compliance incidents must be reported to the FISC in either an immediate notice or (for less significant incidents) in a quarterly report.³⁴⁰ Rule 13(b) states that such reports must include a description of the incident of noncompliance, the facts and circumstances related to the incident, any modifications that will be made in how the government is using the authority in light of the incident, and a description of how the government will handle any information obtained as a result of the incident.³⁴¹ In addition, but separately, the Attorney General and Director of National Intelligence must semiannually jointly conduct an assessment regarding the agencies' compliance with their targeting procedures, minimization procedures, and the Attorney General Guidelines.³⁴² This semiannual assessment must be provided to the Congressional Committees and to the FISC.³⁴³ To date, four of the semiannual assessments have been partially declassified and are publicly available.³⁴⁴

To meet these various reporting obligations, a team of NSD and ODNI personnel review incident reports, request additional information, and (when necessary) further investigate potential incidents of noncompliance.³⁴⁵ These inquiries and investigations entail frequent interaction with counterparts in the internal agency compliance programs discussed above. In addition to resolving individual compliance matters, the NSD and ODNI team lead weekly calls and bimonthly meetings with representatives from the NSA, CIA, and FBI to discuss, among other things, compliance trends and incidents that affect multiple agencies.³⁴⁶

³³⁸ See 50 U.S.C. § 1881f(b)(1)(G); FISC Rule of Procedure 13(b).

³³⁹ 50 U.S.C. § 1881f(b)(1)(G).

³⁴⁰ See MAY 2010 SEMIANNUAL ASSESSMENT, *supra* at 22 (discussing requirements under Rule 10(c), the predecessor to Rule 13(b) in the prior set of FISC Rules of Procedure); NSA DCLPO REPORT, *supra*, at 3 (discussing individual notices and quarterly reports).

³⁴¹ FISC Rule of Procedure 13(b).

³⁴² 50 U.S.C. § 1881a(l)(1).

³⁴³ 50 U.S.C. § 1881a(l)(1).

³⁴⁴ See SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUES PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, MARCH 2009, *available at* <http://www.dni.gov/files/documents/FAA/SAR%20March%202009%20Final%20Release%20with%20Exemptions.pdf>; SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUES PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, DECEMBER 2009, *available at* <http://www.dni.gov/files/documents/FAA/SAR%20December%202009%20Final%20Release%20with%20Exemptions.pdf>; May 2010 Semiannual Assessment, *supra*; August 2013 Semiannual Assessment, *supra*.

³⁴⁵ MAY 2010 SEMIANNUAL ASSESSMENT, *supra*, at 22.

³⁴⁶ See *generally* AUGUST 2013 SEMIANNUAL REPORT, *supra*, at 11 (discussing bimonthly meetings).

Some of the results of the NSD and ODNI's compliance investigations and reports are discussed below.

D. Inspector General Reports

Section 702 also authorizes inspectors general of agencies that acquire data pursuant to Section 702 to conduct reviews of the Section 702 program.³⁴⁷ The inspectors general are authorized to evaluate the agencies compliance with the targeting procedures, minimization procedures, and Attorney General Guidelines.³⁴⁸ Any such reviews are required to contain an accounting of the number of disseminated reports containing U.S. person identities, the number of instances those identities were unmasked, and the number of targets that were subsequently determined to be located in the United States.³⁴⁹ The results of these reviews must be provided to the Attorney General, Director of National Intelligence, FISC, and the Congressional Committees.³⁵⁰ The NSA and DOJ³⁵¹ Inspectors General have conducted reviews under this provision. The reports of these reviews have not been declassified.

E. FISC Oversight

The FISC's primary role in Section 702 is to review the Section 702 certifications and corresponding targeting and minimization procedures for compliance with the statute and the Fourth Amendment. As is described in detail above, the FISC has held that this review of the Section 702 certifications and related documents cannot be made in a vacuum, but instead must be made in light of the actual manner in which the government has implemented (or plans to implement) the Section 702 authorities. In addition to filings made by the government to the FISC in support of the certifications, the FISC's determinations are informed by the information provided in the NSD's reports of all incidents of noncompliance with the procedures,³⁵² the Attorney General and Director of National Intelligence's semiannual assessment regarding compliance with the procedures,³⁵³ the annual reports of agency heads that conduct Section 702 acquisition,³⁵⁴

³⁴⁷ 50 U.S.C. § 1881a(l)(2).

³⁴⁸ 50 U.S.C. § 1881a(l)(2)(A).

³⁴⁹ 50 U.S.C. § 1881a(l)(2)(B), (C).

³⁵⁰ 50 U.S.C. § 1881a(l)(2)(D).

³⁵¹ See Press Release, Dept. of Justice, Office of the Inspector General, DOJ OIG Issues Report on Activities Under Section 702 of the FISA Amendments Act (Sept. 25, 2012), *available at* http://www.justice.gov/oig/press/2012/2012_09_25.pdf.

³⁵² FISC Rule of Procedure 13(b).

³⁵³ 50 U.S.C. § 1881a(l)(1).

³⁵⁴ 50 U.S.C. § 1881a(l)(3).

and any reports by the inspectors general.³⁵⁵ In reviewing the certifications, the FISC also will order the government to respond in writing to questions regarding the conduct of the Section 702 collection program and holds hearings in order to take sworn testimony from government witnesses.³⁵⁶

The FISC's oversight role is not limited to the renewal of Section 702 certifications. The government's obligation to report incidents of noncompliance under the FISC's rules is independent of whether any Section 702 certification is currently pending before the court.³⁵⁷ In a letter to Senate Judiciary Committee Chairman Patrick Leahy, former FISC Presiding Judge Reggie Walton stated that with respect to all FISA compliance matters, to include incidents of noncompliance with the Section 702 program, the court may seek additional information, issue orders to the government to take specific action to address an incident of noncompliance, or (if deemed necessary) issues orders to the government to cease an action that the court assesses to be non-compliant.³⁵⁸

F. Congressional Oversight

The Senate Select Committee on Intelligence, Senate Committee on the Judiciary, House Permanent Select Committee on Intelligence, and House Judiciary Committee are the committees that oversee the government's use of FISA information, including Section 702 information. In passing the FISA Amendments Act, Congress mandated that the Attorney General provide these four committees with a semiannual report describing several aspects of the Section 702 program and further provide the committees with the underlying documents that govern the program.³⁵⁹ Among other things, this semiannual report must include copies of the reports from any compliance reviews conducted by the DOJ or ODNI, a description of any and all incidents of noncompliance by the Intelligence Community or an electronic communications service provider, any certifications (including targeting and minimization procedures), and the directives sent to the electronic communication service providers.³⁶⁰ The semiannual report must also include a description of the FISC's review of the certifications and copies of any order by the FISC or

³⁵⁵ 50 U.S.C. § 1881a(l)(2).

³⁵⁶ FISC Rules of Procedure 5(c) and 17; Bates October 2011 Opinion, *supra*, at 7-10, 2011 WL 10945618 at *2-4 (examples of filings and hearing described); Letter from Presiding Judge Reggie B. Walton, Foreign Intelligence Surveillance Court to Senator Patrick Leahy, Chairman, Senate Comm. on the Judiciary, at 4-6 (July 29, 2013) ("Judge Walton Letter") (describing government submissions related to Section 702 certifications and the types of additional information sought from the government by the FISA court), available at <http://www.fisc.uscourts.gov/sites/default/files/Correspondence%20Leahy-1.pdf>.

³⁵⁷ FISC Rule of Procedure 13(b).

³⁵⁸ Judge Walton Letter, *supra*, at 10-11.

³⁵⁹ 50 U.S.C. § 1881f.

³⁶⁰ 50 U.S.C. § 1881f(b)(1).

pleading by the government that contains a significant legal interpretation of Section 702.³⁶¹

In practice, the government provides the four committees all government filings, hearing transcripts, and FISC orders and opinions related to the court's consideration of the Section 702 certifications. In addition, the Congressional Committees receive the classified Attorney General and Director of National Intelligence's semiannual assessment regarding compliance with the procedures,³⁶² the annual reports of agency heads that conduct Section 702 acquisition,³⁶³ and any reports by the inspectors general.³⁶⁴

In addition to these statutory requirements, the agencies may separately (and more promptly) inform the Congressional Committees of substantial compliance incidents.³⁶⁵ The committees also hold hearings, and committee members and staff receive briefings, regarding the implementation of the Section 702 program.³⁶⁶

IX. Compliance Issues

The Section 702 program is a technically complex collection program with detailed rules embodied in the targeting procedures, minimization procedures, and Attorney General Guidelines regarding targeting, acquisition, querying, retention, and dissemination. Incidents of noncompliance with these rules have been identified in the course of the oversight conducted by the agencies themselves, by the NSD, and by the ODNI. These internal and external compliance programs have not to date identified any intentional attempts to circumvent or violate the procedures or the statutory requirements,³⁶⁷ but both unintentional incidents of noncompliance and instances where Intelligence Community personnel did not fully understand the requirements of the statute and the procedures have been identified.

The government calculates a compliance incident rate for the Section 702 program by dividing the number of identified compliance incidents by the average number of selectors on task. This incident rate has been substantially below one percent since the

³⁶¹ 50 U.S.C. § 1881f(b)(1)(D). Copies of documents related to significant legal interpretations are also produced to Congress pursuant to 50 U.S.C. § 1871.

³⁶² 50 U.S.C. § 1881a(l)(1).

³⁶³ 50 U.S.C. § 1881a(l)(3).

³⁶⁴ 50 U.S.C. § 1881a(l)(2).

³⁶⁵ *See, e.g.*, NSA DCLPO REPORT, *supra*, at 3.

³⁶⁶ *See, e.g.*, S. Rep. No. 112-174, at 2 (2012).

³⁶⁷ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 23.

Section 702 program was initiated. The most common type of compliance incident that has occurred has involved instances in which the NSA otherwise complied with the targeting and minimization procedures in tasking and detasking a selector, but failed to make a report to the NSD and ODNI in the time frame required by the NSA targeting procedures.³⁶⁸ Such notification delays made up over half of the reported incidents in the most recently declassified Attorney General/Director of National Intelligence semiannual assessment.³⁶⁹ Two other common reasons compliance incidents occurred have been that (1) the wrong selector was tasked due to a typographical error,³⁷⁰ or (2) a delay in detasking resulted when an analyst detasked some, but not all, of the Section 702–tasked selectors used by a non-U.S. person target known to be traveling to the United States.³⁷¹ Taken together, these three errors accounted for almost 75% of the compliance incidents that occurred during the reporting period of the most recently declassified Attorney General/Director of National Intelligence semiannual assessment.

Less common incidents, however, can have greater privacy implications. For example, the NSA has reported instances in which the NSA analysts conducted queries of Section 702–acquired data using U.S. person identifiers without receiving the proper approvals because the analyst either did not realize that the NSA knew the identifier to be used by a U.S. person or the analyst mistakenly queried Section 702–acquired data after receiving approvals to use a U.S. person identifier to query other non-Section 702–acquired data.³⁷²

In addition to such human errors, technical issues can lead to overcollection incidents. For example, the government has disclosed that technical errors have resulted in delays in detasking selectors found to be used by persons located in the United States.³⁷³ The government has also disclosed that both changes in how communications transit the telecommunications system and design flaws in the systems the government uses to acquire such communications can, and have, resulted in the acquisition of data beyond what was authorized by Section 702 program.³⁷⁴ Such unauthorized collection is required to be purged upon recognition.

³⁶⁸ See, e.g., AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 23-24.

³⁶⁹ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 26.

³⁷⁰ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 33 n.21.

³⁷¹ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 33.

³⁷² AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 30.

³⁷³ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 32.

³⁷⁴ AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 31-32 (stating that an undisclosed number of “incidents” involving overcollection as a result of changes in the global telecommunications environment, unforeseen consequences of software modifications, or system design issues occurred during the reporting period).

Several systemic incidents have also occurred in the government's operation of the Section 702 program. As is described above, the government's upstream acquisition of multi-communication transactions led to substantial modifications of the NSA minimization procedures and the purging of several years of prior collection. In an earlier incident, the NSA discovered that its practices for executing purges were substantially incomplete. Modifications to better tag, track, and purge data from the NSA's systems when required were implemented.

More recently, questions raised by the NSD/ODNI oversight team led to the discovery that post-tasking checks used to identify indications that a target is located in the United States were incomplete or, for some selectors, non-existent for over a year. After this issue was discovered, the relevant systems were modified to correct several errors, efforts were made to identify travel to the United States that had been previously missed (and corresponding purges were conducted), and additional modifications to the agencies' minimization procedures were made to ensure that data acquired while a Section 702 target had traveled to the United States will not be used.

Since the Section 702 program's inception, the compliance programs have also identified two instances of reverse targeting. The first instance, which was discovered by the NSD/ODNI targeting review, involved the reverse targeting of a non-U.S. person located inside the United States in order to acquire foreign intelligence information. The second, which involved reverse targeting to acquire information about a U.S. person located outside the United States, was identified by NSA oversight personnel. The targeting in the first incident resulted in the acquisition of communications that were subsequently purged; the targeting in the second incident did not result in any communications being acquired. In both incidents, the analysts who engaged in the reverse targeting substantially misunderstood the prohibition against reverse targeting. Given the centrality of this prohibition to Section 702 targeting, these analysts were retrained not only on the reverse targeting prohibition, but on other fundamental targeting requirements.

Part 4:

LEGAL ANALYSIS

I. Overview

Part Four is divided into three sections: Statutory Analysis, Constitutional Analysis, and Analysis of Treatment of Non-U.S. Persons. The Statutory Analysis section explains the statutory framework for collection under Section 702 of the Foreign Intelligence Surveillance Act (“FISA”) and provides the Board’s evaluation of whether PRISM and upstream collection comply with the statute. The Constitutional Analysis section details the Board’s evaluation of the constitutionality of the program — examining the warrant requirement and its exceptions, and assessing the program’s reasonableness under the Fourth Amendment. Part Four concludes with a discussion of the treatment of non-U.S. persons under the program.

II. Statutory Analysis

A. Establishment of Section 702

As noted in the Board’s Report on the Section 215 program, FISA was enacted in 1978 to establish a procedure under which the Attorney General could obtain a judicial order authorizing the use of electronic surveillance in the United States for foreign intelligence purposes. Its original provisions — now referred to as “traditional FISA” — authorized, among other things, individualized FISA orders for electronic surveillance relating to a specific person, place, or communications account or device.

Over time, Congress has enacted legislation bringing additional categories of foreign intelligence gathering within FISA’s ambit. One of the latest examples of this is the enactment of the FISA Amendments Act of 2008.³⁷⁵ As outlined in Part 3 of this Report, the FISA Amendments Act, which includes the new Section 702 of FISA, replaced the temporary authority of the Protect America Act, which in turn, was designed to codify part of the President’s Surveillance Program. The statute was enacted in response to Congress’ conclusion that FISA should be amended to provide a separate procedure to facilitate the targeting of persons reasonably believed to be outside the United States to acquire foreign intelligence information.³⁷⁶ This statute was developed during a time of public debate and

³⁷⁵ Pub. L. No. 110-261, 122 Stat. 2436 (2008).

³⁷⁶ S. Rep. No. 110-209, at 2 (2007).

concern regarding the intelligence activities undertaken by the government, and it was an attempt to put a statutory framework around activities that were currently ongoing.³⁷⁷

As discussed below, the government utilizes two collection methods under Section 702 — PRISM collection and upstream collection (which includes acquiring “about” communications). The manner in which collection is effectuated via PRISM and upstream varies; therefore, the Board has analyzed the statutory compliance of each collection method separately. After reviewing the operation of the Section 702 program as a whole, and each collection method implemented under Section 702 individually, the Board has concluded that PRISM collection is expressly authorized by the statute and that the statute, while silent on “about” upstream collection, can permissibly be interpreted as allowing such collection as currently implemented.

B. Collection Under Section 702

1. Statutory Framework for Collection

Congress created Section 702 to authorize Foreign Intelligence Surveillance Court (“FISC” or “FISA court”) approval of certifications which authorize the acquisition of broad *categories* of foreign intelligence information through the targeting of non-U.S. persons reasonably believed to be located outside the United States.³⁷⁸ A non-U.S. person is an individual who is neither a citizen nor a lawful permanent resident of the United States. As described in detail in Part 3 of this Report, the Attorney General and the Director of National Intelligence must submit a certification to and receive an order from the FISA court that permits them to authorize the targeting.³⁷⁹

Under Section 702, the FISC has the authority to review the government’s certifications, targeting procedures, and minimization procedures, and the court must approve these certifications and procedures under criteria set forth in the statute. The FISC does not review specific selectors³⁸⁰ tasked for collection nor does it review the *individual* factual basis for expecting that the tasking of a particular selector will result in the acquisition of foreign intelligence information. In its review and approval process, however, the FISC has the authority to do more than a rote check to ensure that the government meets its statutory requirements. The FISC’s mandate to ensure compliance with the Fourth Amendment is expressly enumerated in the statute, and the court has required the government to make changes to its collection under Section 702 in the past on

³⁷⁷ See S. Rep. No. 110-209, at 5 (2007).

³⁷⁸ See 50 U.S.C. § 1881a(a), (g).

³⁷⁹ 50 U.S.C. § 1881a(a), (g), (i).

³⁸⁰ A selector is a unique identifier associated with a *particular* individual or entity. See pages 32-33 of this Report.

this basis.³⁸¹ Additionally, the FISA court has an oversight role: the FISC Rules of Procedure impose an ongoing duty on the government to immediately correct any misstatement or omission of material facts that it has provided to the court, as well as to disclose any instance in which the government's conduct did not comply with the FISC's authorization or with applicable law.³⁸²

On the whole, Section 702 provides the public with transparency into the legal framework for collection and publicly outlines the basic structure of the program. Use of the words "target" and "targeting" allowed Congress to signal the type of collection activity undertaken by the government without detailing operational methods and tactics. In addition, it is clear from the face of the statute that the government must submit certifications to the FISC as well as implement targeting and minimization procedures that have been approved by the court.

2. PRISM Collection

The Board concludes that as currently implemented, the operation of PRISM collection falls within the framework of the statute. Section 702 expressly authorizes the "targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." As described in Part 3 above, under PRISM collection the government acquires communications to and from approved targets using communications "selectors" that are associated with particular persons. Examples of communications selectors include email addresses, but not key words.³⁸³ The collection of communications to and from a target inevitably returns communications in which non-targets are on the other end, some of whom will be U.S. persons.³⁸⁴ Such "incidental" collection of communications is not accidental, nor is it inadvertent.³⁸⁵

The incidental collection of communications between a U.S. person and a non-U.S. person located outside the United States, as well as communications of non-U.S. persons outside the United States that may contain information about U.S. persons, was clearly

³⁸¹ See Memorandum Opinion, [*Caption Redacted*], [Docket No. Redacted], 2011 WL 10945618 (FISA Ct. Oct. 3, 2011) ("Bates October 2011 Opinion"), available at <http://icontherecord.tumblr.com/post/58944252298/dni-declassifies-intelligence-community-documents>.

³⁸² United States Foreign Intelligence Surveillance Court Rules of Procedure, Rule 13, available at <http://www.uscourts.gov/uscourts/rules/FISC2010.pdf>.

³⁸³ Privacy and Civil Liberties Oversight Board, Transcript of Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, at 26 (Mar. 19, 2014) ("PCLOB March 2014 Hearing Transcript") (statement of Rajesh De, General Counsel, NSA), available at http://www.pcllob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/19-March-2014_Public_Hearing_Transcript.pdf.

³⁸⁴ PCLOB March 2014 Hearing Transcript, *supra*, at 96-97 (statement of Robert Litt, General Counsel, ODNI).

³⁸⁵ PCLOB March 2014 Hearing Transcript, *supra*, at 96-97.

contemplated by Congress at the time of drafting. The statute prohibits the targeting of U.S. persons, but not the incidental acquisition of communications involving U.S. persons. Further, the statute requires the government to adopt procedures that, among other things, are reasonably designed to minimize (not eliminate) the acquisition and retention of private information about U.S. persons, consistent with the government's foreign intelligence needs.³⁸⁶ The statute also calls for the Department of Justice and the Intelligence Community to review and report on disseminations of U.S. person information, including cases in which the U.S. person is not referred to by name.³⁸⁷ The Senate Select Committee on Intelligence has explained the inevitability of such incidental collection and how Congress responded to that inevitability:

Congress recognized at the time the FISA Amendments Act was enacted that it is simply not possible to collect intelligence on the communications of a party of interest without also collecting information about the people with whom, and about whom, that party communicates, including in some cases non-targeted U.S. persons . . .

Specifically, in order to protect the privacy and civil liberties of U.S. persons, Congress mandated that, for collection conducted under Section 702, the Attorney General adopt, and the FISA Court review and approve, procedures that minimize the acquisition, retention, and dissemination of nonpublicly available information concerning unconsenting U.S. persons.³⁸⁸

Based on the information that the Board has reviewed, the government's PRISM collection complies with the structural requirements of the statute. As outlined above, the government has filed certifications authorizing the acquisition of certain categories of targets with the FISA court and has developed and submitted for FISA court approval targeting and minimization procedures as required by the statute. Incidentally collected U.S. person information is subject to these minimization procedures that set standards for acquisition and retention of information and permit disseminations of U.S. person information only for a foreign intelligence purpose or when the information is evidence of a crime.³⁸⁹ After a thorough review, the Board has concluded that the government generally is complying with the targeting limitations set forth in subsections (b)(1) through (b)(4) and has adopted Attorney General guidelines that, among other things, prohibit reverse

³⁸⁶ See 50 U.S.C. §§ 1801(h), 1881a(e).

³⁸⁷ See 50 U.S.C. § 1881a(l)(2), (3).

³⁸⁸ S. Rep. No. 112-174, at 8 (2012).

³⁸⁹ See 50 U.S.C. §§ 1801(h), 1881a(e).

targeting. Although there have been documented compliance incidents,³⁹⁰ we conclude that overall PRISM collection falls within the framework of the statute.

3. Upstream Collection

As described above, upstream collection constitutes a small percentage of collection under Section 702. To the extent that upstream collection involves acquiring communications to and from targeted persons, it fits within the statutory framework in the same way that PRISM collection does. Targeting under PRISM and upstream collection work in the same way; the mode of collection is different.

Upstream collection under Section 702 poses an additional question for statutory analysis because, as described above in Part 3, the upstream process captures not only communications to and from targeted persons, but also other communications that contain reference to the selector of a targeted person — which are referred to as “about” communications.³⁹¹

The statutory language of Section 702 does not expressly permit or prohibit collection of communications “about” a target. 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. Indeed, the words “target” and “targeting” are not defined in either the original version of FISA or the FISA Amendments Act despite being used throughout the statute. Some commenters have questioned whether the collection of such “about” communications complies with the statute. We conclude that Section 702 may permissibly be interpreted to allow “about” collection as it is currently conducted.

Collection of “about” communications occurs only in upstream collection, not in PRISM.³⁹² Unlike PRISM collection, upstream collection acquires “Internet transactions,” meaning packets of data that traverse the Internet, directly from the Internet “backbone.”³⁹³ Utilizing this method, the government is able to capture communications that contain an approved selector, no matter where it appears in the communication — whether in the “to” or “from” lines of an email, for instance, or in the body of the email.

As discussed in Part 3 above, there are technical reasons why “about” collection is needed to acquire even some communications that are “to” and “from” a target. Some other

³⁹⁰ See pages 77-79 of this Report.

³⁹¹ PCLOB March 2014 Hearing Transcript, *supra*, at 26.

³⁹² PCLOB March 2014 Hearing Transcript, *supra*, at 63.

³⁹³ PCLOB March 2014 Hearing Transcript, *supra*, at 26; Bates October 2011 Opinion, *supra*, at 27-28 & n.23, 2011 WL 10945618, at *9 & n.23.

types of “about” communications also involve Internet activity of the actual target. For some communications, the NSA’s collection devices are not able to distinguish between communications that are actually “to” or “from” a target and those in which the selector is found in the body of a communication, nor can they distinguish among the different types of “about” communications. Thus, under current technology and program design, in order to avoid significant gaps in upstream collection coverage, “about” collection is largely a technical inevitability.³⁹⁴

As a result, if the selector is contained within the body of a communication, “about” collection may result in the acquisition of communications between two non-targets. In some such instances, both of the individuals who are parties to the communication could be U.S. persons or persons located within the United States. This occurs because the current state of technology renders the government unable to determine with certainty the location of all communicants at the time of acquisition.

In addition, upstream collection leads to the acquisition of multi-communication transactions (“MCTs”).³⁹⁵ As explained in Part 3 above, MCTs that contain a communication to, from, or about a target may be embedded within communications that are between U.S. persons or persons located within the United States, and the government has not been able to design a filter that would acquire only the single discrete communications within transactions that contain a selector.

Thus, due to the inclusion of “about” collection and the collection of MCTs, there is a greater risk that the NSA will acquire purely domestic communications through upstream collection than through PRISM. This risk is mitigated to some extent by the fact that through the upstream process, Internet transactions are first filtered to help eliminate potential domestic transactions before they are screened to determine whether a transaction contains a tasked selector. Further, NSA’s minimization procedures include more stringent safeguards for upstream data than they do for PRISM data. In particular, the NSA, the only agency that conducts upstream collection and the only agency that has access to unminimized results of upstream collection, is not permitted to use U.S. person identifiers in conducting queries of the upstream data. In addition, the retention period for

³⁹⁴ As a general rule, in conducting traditional wiretaps, the government has been permitted to access a trunk line if it has no reasonable physical access to a particular line or device, subject to strict limits on retention and use of non-targeted communications.

³⁹⁵ The acquisition of MCTs through the upstream collection process, and the minimization procedures adopted to address the specific challenges posed by acquisition of MCTs, are described in detail in Part 3 of this Report. The constitutional and policy questions raised by the collection of MCTs are addressed in those respective sections of this Report.

Internet communications collected through upstream is two years, as opposed to the NSA's five-year retention period for data collected in PRISM.³⁹⁶

Given the lack of any textual prohibition, as well as the present technical necessity of capturing "about" communications in certain circumstances as part of the upstream collection process, we conclude that the inclusion of "about" collection under the current operation of the program is a permissible reading of the statute.

III. Constitutional Analysis

Evaluating the constitutionality of the Section 702 program poses unique challenges. Unlike the typical Fourth Amendment inquiry, where the legitimacy of "a particular search or seizure" is judged "in light of the particular circumstances" of that case,³⁹⁷ evaluating the government's implementation of Section 702 requires assessing a complex surveillance *program* — one that entails many separate decisions to monitor large numbers of individuals, resulting in the annual collection of hundreds of millions of communications of different types, obtained through a variety of methods, pursuant to multiple foreign intelligence imperatives, and involving four intelligence agencies that each have their own rules governing how they may handle and use the communications that are acquired.³⁹⁸

Further complicating the analysis, the constitutional interests at stake are not those of the persons targeted for surveillance under Section 702, all of whom lack Fourth Amendment rights because they are foreigners located outside of the United States.³⁹⁹

³⁹⁶ 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, § 3(c) (Oct. 31, 2011) ("NSA 2011 Minimization Procedures").

³⁹⁷ *Scott v. United States*, 436 U.S. 128, 137 (1978).

³⁹⁸ Most *programs* of searches or seizures that have been evaluated under the Fourth Amendment have involved uniform practices that advanced a single government interest through standardized means that intruded upon the privacy interests of each person affected in the same manner. *See, e.g., Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646 (1995) (drug testing of student athletes); *Michigan Dep't of State Police v. Sitz*, 496 U.S. 444 (1990) (highway sobriety checkpoints). Courts also sometimes undertake programmatic assessments in response to statutory facial challenges, where they evaluate "the constitutionality of a statute without factual development centered around a particular application." *In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1009 (FISA Ct. Rev. 2008) (citing *Wash. State Grange v. Wash. State Repub. Party*, 128 S. Ct. 1184, 1190 (2008)). Here, however, the Board has not asked whether Section 702 "is valid on its face — a question that would be answered by deciding whether *any* application of the statute passed constitutional muster." *Id.* at 1009-10. Instead, it has asked whether "this specific application" of the statute — the program as it is conducted today — is consistent with the Constitution. *Id.* at 1010.

³⁹⁹ *See United States v. Verdugo-Urquidez*, 494 U.S. 259, 274-75 (1990) (holding that the Fourth Amendment has no application to a physical search in a foreign country of the residence of a citizen of that country who has no voluntary attachment to the United States).

Instead, the relevant Fourth Amendment interests are those of the U.S. persons whose communications may be acquired despite not themselves having been targeted for surveillance.⁴⁰⁰

Although U.S. persons and other persons in the United States may not be targeted under Section 702, operation of the program nevertheless results in the government acquiring some telephone and Internet communications involving U.S. persons, potentially in large numbers. As explained above, this acquisition can occur in four main situations:

- (1) A U.S. person communicates by telephone or Internet with a foreigner located abroad who has been targeted. The government refers to this as “incidental” collection.
- (2) A U.S. person sends or receives an Internet communication that is routed internationally and that includes a reference to a selector such as an email address used by a foreigner who has been targeted. The government refers to this as “about” collection.⁴⁰¹
- (3) A U.S. person sends or receives an Internet communication that is embedded within the same “transaction” as a different communication that meets the requirements for acquisition (because it is to or from a targeted foreigner or includes a reference to the communications identifier of a targeted foreigner). The government refers to these transactions containing more than one separate communication as “multiple-communication transactions” or “MCTs.”⁴⁰²
- (4) A U.S. person’s communications are acquired by mistake due to a targeting error, an implementation error, or a technological malfunction. The government refers to this as “inadvertent” collection.

Any Fourth Amendment assessment of the Section 702 program must take into account the cumulative privacy intrusions and risks of all four categories above, together with the limits and protections built into the program that mitigate them.⁴⁰³

⁴⁰⁰ In addition to U.S. persons, foreign citizens temporarily and voluntarily present within the United States likely possess Fourth Amendment rights. *See Verdugo-Urquidez*, 494 U.S. at 278 (Kennedy, J., concurring).

⁴⁰¹ See pages 37-39 of this Report for an explanation of “about” collection.

⁴⁰² See pages 39-41 of this Report for a discussion of “MCTs.”

⁴⁰³ Apart from these four categories, there is of course a risk that government personnel could deliberately misuse the Section 702 program to target a U.S. person for surveillance. Doing so would be grounds for professional sanction and possibly criminal prosecution, however, and auditing procedures are in place to deter such wrongdoing. Every targeting decision made by an analyst is recorded and reviewed both by supervisors within the NSA and also by a joint oversight team from the Department of Justice and Office of

After analyzing these factors, the Board finds that the core of this 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 communicate foreign intelligence, using specific communications identifiers, subject to FISA court-approved targeting rules that have proven to be accurate in targeting persons outside the United States, and subject to multiple layers of rigorous oversight — fits within the totality of the circumstances test for reasonableness as it has been defined by the courts to date. Outside of this fundamental core, certain aspects of the Section 702 program push the entire program close to the line of constitutional reasonableness. Such aspects include the scope of the incidental collection of U.S. persons’ communications, the use of “about” collection to acquire Internet communications that are neither to nor from the target of surveillance, and the use of queries to search the information collected under the program for the communications of specific U.S. persons. With these concerns in mind, this Report offers a set of policy proposals designed to push the program more comfortably into the sphere of reasonableness, ensuring that the program remains tied to its constitutionally legitimate core.

A. Privacy in Telephone and Internet Communications

The Fourth Amendment protects the right of the people “to be secure in their persons, houses, papers, and effects.” It thus prohibits “unreasonable searches and seizures” by the government, and it specifies that a warrant authorizing a search or seizure may issue only “upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”⁴⁰⁴ A search occurs not only where the government intrudes on a person’s tangible private property to obtain information, but also where “the government violates a subjective expectation of privacy that society recognizes as reasonable.”⁴⁰⁵

Because individuals who are protected by the Constitution have a reasonable expectation of privacy in their telephone conversations, it has long been the rule that wiretapping conducted within the United States for criminal or other domestic purposes is presumptively unreasonable under the Fourth Amendment unless the government has obtained a warrant based on probable cause.⁴⁰⁶ While the Supreme Court has not expressly

the Director of National Intelligence. To date, there are no known instances in which government personnel deliberately violated the statute, targeting procedures, or minimization procedures. There have, however, been instances in which analysts have made mistakes of law, including two instances of reverse targeting. See page 79 of this Report.

⁴⁰⁴ U.S. Const. amend. IV.

⁴⁰⁵ *Kyllo v. United States*, 533 U.S. 27, 33 (2001) (citing *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)); see *United States v. Jones*, 132 S. Ct. 945, 949-50 (2012).

⁴⁰⁶ *Katz*, 389 U.S. at 352-59; see *Arizona v. Gant*, 556 U.S. 332, 338 (2009).

ruled on the extent of Fourth Amendment protection for Internet communications, lower courts have concluded that emails are functionally analogous to mailed letters and that therefore their contents cannot be examined by the government without a warrant.⁴⁰⁷ The same may be true for other, similarly private forms of Internet communication, although this question awaits further development by the courts.

B. Foreign Intelligence Exception to the Warrant Requirement

Under the authority of Section 702, the government collects telephone and Internet communications without obtaining individual judicial warrants for the specific people it targets. Decisions about which telephone and Internet communications to collect are made by executive branch personnel without court review. While the FISC plays a role in overseeing the categories of foreign intelligence the government seeks, the procedures it employs, and its adherence to statutory and constitutional limits, the court has no part in approving individual targeting decisions.

“Although as a general matter, warrantless searches are *per se* unreasonable under the Fourth Amendment, there are a few specifically established and well-delineated exceptions to that general rule.”⁴⁰⁸ And while wiretapping and other forms of domestic electronic surveillance generally require a warrant, the Supreme Court has left open the question of whether “safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security” and “the activities of foreign powers.”⁴⁰⁹

In other words, there may be a “foreign intelligence exception” to the warrant requirement permitting the executive branch to conduct wiretapping and other forms of electronic surveillance without judicial approval. The Supreme Court has not decided whether such an exception exists, in part because the 1978 enactment of the Foreign Intelligence Surveillance Act (“FISA”) forestalled the question: the Act established a framework for foreign intelligence surveillance under which the executive branch obtains

⁴⁰⁷ See *United States v. Warshak*, 631 F.3d 266, 285-86 (6th Cir. 2010) (stating that “[g]iven the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection,” and holding that government agents must obtain a warrant based on probable cause before compelling an Internet service provider to turn over the contents of a subscriber’s emails); *United States v. Maxwell*, 45 M.J. 406, 418 (C.A.A.F. 1996) (holding that “the transmitter of an e-mail message enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant.”); Bates October 2011 Opinion, *supra*, at 73-74, 2011 WL 10945618, at *26 (“A person’s ‘papers’ are among the four items that are specifically listed in the Fourth Amendment as subject to protection against unreasonable search and seizure. Whether they are transmitted by letter, telephone or e-mail, a person’s private communications are akin to personal papers.”).

⁴⁰⁸ *City of Ontario, Cal. v. Quon*, 560 U.S. 746, 760 (2010) (quoting *Katz*, 389 U.S. at 357) (internal quotation marks omitted).

⁴⁰⁹ *Katz*, 389 U.S. at 358 n.23; *United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div.*, 407 U.S. 297, 308 (1972) (“*Keith*”).

warrant-like orders from the FISA court before engaging in surveillance that falls within the ambit of the statute.⁴¹⁰

While the Supreme Court has not spoken, lower courts evaluating surveillance conducted before the enactment of FISA addressed the existence of a foreign intelligence exception, and every court to decide the question recognized such an exception.⁴¹¹ More recently the Foreign Intelligence Surveillance Court of Review concluded that a foreign intelligence exception permitted warrantless surveillance “directed at a foreign power or an agent of a foreign power” — which could include U.S. citizens — under the Protect America Act, a predecessor to Section 702.⁴¹²

This precedent does not neatly resolve all questions about the existence and scope of a foreign intelligence exception to the warrant requirement.⁴¹³ The Board takes no position here on the existence or scope of that exception. We note that the program’s intrusion on U.S. persons’ privacy is reduced by its focus on targeting individually selected foreigners located outside the United States from whom the government reasonably

⁴¹⁰ See 50 U.S.C. §§ 1801-1812; *In re Terrorist Bombings of U.S. Embassies in E. Africa*, 552 F.3d 157, 161 (2d Cir. 2008).

⁴¹¹ See *United States v. Truong Dinh Hung*, 629 F.2d 908, 913 (4th Cir. 1980); *United States v. Buck*, 548 F.2d 871, 875 (9th Cir. 1977); *United States v. Butenko*, 494 F.2d 593, 605 (3d Cir. 1974); *United States v. Brown*, 484 F.2d 418, 426 (5th Cir. 1973); but see *Zweibon v. Mitchell*, 516 F.2d 594, 618-20 (D.C. Cir. 1975).

It is not necessarily clear that the Section 702 program would fall within the *scope* of the foreign intelligence exception recognized by these decisions, which were limited to surveillance directly authorized by the Attorney General, targeting foreign powers or their agents, and/or pursuing foreign intelligence as the primary or sole purpose of the surveillance. See *Truong Dinh Hung*, 629 F.2d at 912-16 (approving surveillance authorized by Attorney General “only if [the executive] is attempting primarily to obtain foreign intelligence from foreign powers or their assistants”); *Buck*, 548 F.2d at 875 (approving surveillance “expressly authorized by the Attorney General”); *Butenko*, 494 F.2d at 596, 606 (approving surveillance “concerning activities within the United States of foreign powers” where “the primary purpose of these searches is to secure foreign intelligence information”); *Brown*, 484 F.2d at 421 (approving “electronic surveillance authorized by the Attorney General and made solely for the purpose of gathering foreign intelligence”). Under Section 702, targets are selected by NSA personnel without Attorney General approval, and they need not be foreign powers or their agents; foreign intelligence need only be “a significant purpose” of the surveillance. See 50 U.S.C. § 1881a(a), (g)(2)(A)(v).

Critically, however, Section 702 targets cannot be U.S. persons or anyone located in the United States. Moreover, limits expressed in pre-FISA opinions addressing the president’s *inherent* and unilateral constitutional power to conduct foreign intelligence surveillance do not necessarily apply to executive implementation of a congressionally enacted statute that involves oversight by all three branches of government. See *United States v. Abu-Jihaad*, 630 F.3d 102, 121 (2d Cir. 2010).

⁴¹² See *In re Directives*, 551 F.3d at 1010-12.

⁴¹³ Apart from the distinctions noted above, nearly all of the relevant decisions predated the implementation of FISA’s surveillance framework beginning in 1978, and experience with FISA and the FISA court since then arguably undermines some of the rationales underlying the foreign intelligence exception, such as the fear that a warrant requirement will unduly “reduce the flexibility of executive foreign intelligence initiatives” and that the judiciary is ill-suited to address “the delicate and complex decisions that lie behind foreign intelligence surveillance.” *Truong Dinh Hung*, 629 F.2d at 913.

expects to obtain foreign intelligence — and by the government’s employment of oversight mechanisms to help ensure adherence to those limitations. Unlike the warrantless surveillance of the pre-FISA era, U.S. persons and others in the United States cannot be targeted under this program, and therefore the government never will be permitted to collect and retain their entire communications history.⁴¹⁴ Instead, the government will have access only to those scattered communications that occur between a U.S. person and a targeted overseas foreigner, or that are acquired through “about” collection or as part of an MCT (which are subject to special limitations on retention and use). Moreover, the fact that the people targeted under Section 702 are situated in foreign countries may often make it difficult and time-consuming for the government to assemble documentation about them sufficient to obtain independent judicial approval for surveillance — while those targets’ lack of Fourth Amendment rights militates against any legal obligation to obtain such approval or to strictly limit targeting to foreign powers and their agents.

C. The “Reasonableness” Framework

“Even if a warrant is not required, a search is not beyond Fourth Amendment scrutiny; for it must be reasonable in its scope and manner of execution.”⁴¹⁵ Thus, “even though the foreign intelligence exception applies in a given case, governmental action intruding on individual privacy interests must comport with the Fourth Amendment’s reasonableness requirement.”⁴¹⁶ The absence of a warrant requirement simply means that, “rather than employing a *per se* rule of unreasonableness,” privacy concerns and governmental interests must be balanced to determine if the intrusion is reasonable.⁴¹⁷

“Whether a search is reasonable,” therefore, “is determined by assessing, on the one hand, the degree to which it intrudes upon an individual’s privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.”⁴¹⁸ Making this determination requires considering the “totality of the circumstances.”⁴¹⁹

Applying this test to a program of intelligence gathering demands “sensitivity both to the government’s right to protect itself from unlawful subversion and attack and to the

⁴¹⁴ If a U.S. person or someone located in the United States is inadvertently targeted based on an erroneous belief about that person’s nationality or location, all of the communications acquired through that targeting must be destroyed, unless, for example, the Director or Acting Director of the NSA specifically determines in writing that an individual communication should be retained because it satisfies one of four criteria. See pages 49-50 of this Report.

⁴¹⁵ *Maryland v. King*, 133 S. Ct. 1958, 1970 (2013).

⁴¹⁶ *In re Directives*, 551 F.3d at 1012 (citing *United States v. Place*, 462 U.S. 696, 703 (1983)).

⁴¹⁷ *King*, 133 S. Ct. at 1970 (quoting *Illinois v. McArthur*, 531 U.S. 326, 331 (2001)).

⁴¹⁸ *Samson v. California*, 547 U.S. 843, 848 (2006) (internal quotation marks omitted).

⁴¹⁹ *Samson*, 547 U.S. at 848.

citizen's right to be secure in his privacy against unreasonable government intrusion."⁴²⁰ When considering surveillance directed at national security threats, particularly those of a foreign nature, it is appropriate to "begin the inquiry by noting that the President of the United States has the fundamental duty, under Art. II, s 1, of the Constitution, to 'preserve, protect and defend the Constitution of the United States,'" and that "[i]mplicit in that duty is the power to protect our government against those who would subvert or overthrow it by unlawful means."⁴²¹ More broadly, the government's interest in protecting national security "is of the highest order of magnitude."⁴²²

Additional consideration is due to the fact that the executive branch, acting under Section 702, is not exercising its Article II power unilaterally, but rather is implementing a statutory scheme enacted by Congress after public deliberation regarding the proper balance between the imperatives of privacy and national security. By establishing a statutory framework for surveillance conducted within the United States but exclusively targeting overseas foreigners, subject to certain limits and oversight mechanisms, "Congress sought to accommodate and advance both the government's interest in pursuing legitimate intelligence activity and the individual's interest in freedom from improper government intrusion."⁴²³ The framework of Section 702, moreover, includes a role for the judiciary in ensuring compliance with statutory and constitutional limits, albeit a more circumscribed role than the approval of individual surveillance requests. Where, as here, "the powers of all three branches of government — in short, the whole of federal authority" — are involved in establishing and monitoring the parameters of an intelligence-gathering activity, the Fourth Amendment calls for a different calculus than when the executive branch acts alone.⁴²⁴

Furthermore, the hostile activities of terrorist organizations and other foreign entities are prone to being geographically dispersed, long-term in their planning, conducted in foreign languages or in code, and coordinated in large part from locations outside the reach of the United States. Accordingly, "complex, wide-ranging, and

⁴²⁰ *Keith*, 407 U.S. at 299 (addressing intelligence gathering aimed at domestic national security threats).

⁴²¹ *Keith*, 407 U.S. at 310.

⁴²² *In re Directives*, 551 F.3d at 1012 (citing *Haig v. Agee*, 453 U.S. 280, 307 (1981)); see *Keith*, 407 U.S. at 312 ("It has been said that '(t)he most basic function of any government is to provide for the security of the individual and of his property.'" (citation omitted)).

⁴²³ *United States v. Cavanagh*, 807 F.2d 787, 789 (9th Cir. 1987) (addressing traditional FISA).

⁴²⁴ *Abu-Jihaad*, 630 F.3d at 121 (addressing traditional FISA); cf. *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 635-38 (1952) (Jackson, J., concurring).

decentralized organizations, such as al Qaeda, warrant sustained and intense monitoring in order to understand their features and identify their members.”⁴²⁵

On the other side of the coin, the acquisition of private communications intrudes on Fourth Amendment interests. Even though U.S. persons and persons located in the United States are subject to having their telephone conversations collected only when they communicate with a targeted foreigner located abroad, the program nevertheless gains access to numerous personal conversations of U.S. persons that were carried on under an expectation of privacy. Email communications to and from U.S. persons, which the FISA court has said are akin to “papers” protected under the Fourth Amendment,⁴²⁶ are also subject to collection in a variety of circumstances. Digital tools enable the government to query the repository of collected communications to locate communications involving a given person in search of foreign intelligence or evidence of a crime.⁴²⁷

D. Holistic Assessment of Reasonableness

As discussed elsewhere in this Report, the Board believes that the Section 702 program significantly aids the government’s efforts to prevent terrorism, as well as to combat weapons proliferation and gather foreign intelligence for other purposes. The question, then, is how the program’s intrusion on the privacy of U.S. persons weighs against its substantial contribution to these governmental interests.⁴²⁸

This evaluation must consider *the program as a whole* — taking into account how and why the communications of U.S. persons are acquired and what is done with them afterward. Thus, the privacy risks posed by the comparatively broad scope of targeting under this program and the absence of individual warrants must be offset by the applicable rules restricting the acquisition, use, dissemination, and retention of the communications that are acquired. In this regard, we must consider whether practices that permit use of U.S.

⁴²⁵ *In re Terrorist Bombings*, 552 F.3d at 175 (citing *In re Sealed Case*, 310 F.3d 717, 740-41 (FISA Ct. Rev. 2002)).

⁴²⁶ *See* Bates October 2011 Opinion, *supra*, at 74, 2011 WL 10945618, at *26 (“[T]he Supreme Court has held that the parties to telephone communications and the senders and recipients of written communications generally have a reasonable expectation of privacy in the contents of those communications The intrusion resulting from the interception of the contents of electronic communications is, generally speaking, no less substantial.”). Since the nineteenth century, in order to protect the security of personal papers and effects, the Supreme Court has held that the government cannot engage in a warrantless search of the contents of sealed mail. *Ex parte Jackson*, 96 U.S. 727, 733 (1877) (“Letters . . . in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles.”). The Sixth Circuit Court of Appeals has held that email enjoys constitutional protection no less than physical letters. *Warshak*, 631 F.3d at 284-86.

⁴²⁷ *See* pages 55-60 of this Report for a description of the rules and procedures governing queries.

⁴²⁸ *See Samson*, 547 U.S. at 848.

persons' communications after their collection are appropriate given the less rigorous rules on targeting that permitted their acquisition.

This holistic approach is consistent with available precedent. When evaluating governmental policies authorizing warrantless searches or seizures, the Supreme Court has indicated that limits on the uses to which the collected information may be put, and on access to that information, bear on the policy's reasonableness under the Fourth Amendment.⁴²⁹ Lower courts addressing the traditional FISA process have similarly noted that, despite its somewhat more lenient requirements compared with traditional criminal wiretaps, it safeguards privacy rights through "an expanded conception of minimization that differs from that which governs law-enforcement surveillance."⁴³⁰ The Foreign Intelligence Surveillance Court of Review, addressing a surveillance program with similarities to Section 702, emphasized the "matrix of safeguards" governing the program, including "effective minimization procedures" that "serve[d] as an additional backstop against identification errors as well as a means of reducing the impact of incidental intrusions into the privacy of non-targeted United States persons."⁴³¹ The FISA court has applied this approach to Section 702, having "recognized that the procedures governing retention, use, and dissemination bear on the reasonableness under the Fourth Amendment of a program for collecting foreign intelligence information."⁴³²

The government has acknowledged that the Fourth Amendment rights of U.S. persons are affected when their communications are acquired under Section 702 incidentally or otherwise, and it has echoed the FISA court's observation that the implementation of adequate minimization procedures is part of what makes the collection reasonable.⁴³³

⁴²⁹ See, e.g., *King*, 133 S. Ct. at 1967 (in approving collection of DNA information from arrestees, ascribing significance to restrictions on the information that may be added to databases and for what purposes it may be used); *Vernonia*, 515 U.S. at 658 (emphasizing that "the results of the [drug] tests [for student athletes] are disclosed only to a limited class of school personnel who have a need to know; and they are not turned over to law enforcement authorities or used for any internal disciplinary function").

⁴³⁰ *United States v. Belfield*, 692 F.2d 141, 148 (D.C. Cir. 1982) (citation omitted).

⁴³¹ *In re Directives*, 551 F.3d at 1013, 1015.

⁴³² See Bates October 2011 Opinion, *supra*, at 77, 2011 WL 10945618, at *27. Exemplifying this approach, when the FISA court concluded that the upstream portion of the program was unreasonably acquiring too many domestic and irrelevant communications through the collection of MCTs, it declared that portion of the program to violate the Fourth Amendment, but it later concluded that the program had returned within constitutional bounds after new procedures were adopted to specially handle those communications. See *id.* at 68-79, 2011 WL 10945618, at *24-28; see also Memorandum Opinion, [*Caption Redacted*], [Docket No. Redacted], 2011 WL 10947772 (FISA Ct. Nov. 30, 2011), available at <http://icontherecord.tumblr.com/post/58944252298/dni-declassifies-intelligence-community-documents>.

⁴³³ See PCLOB March 2014 Hearing Transcript, *supra*, at 15 (statement of Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ) ("That's not to say that U.S. persons whose . . . communications are collected incidentally doesn't trigger a Fourth Amendment review. It does. Those people

An important ramification of this holistic approach is that concerns about post-collection practices such as the use of queries to search for the communications of specific U.S. persons cannot be dismissed on the basis that the communications were “lawfully collected.” Rather, whether Section 702 collection is constitutionally reasonable in the first place, and hence “lawful,” depends on the reasonableness of the surveillance regime as a whole, including whether its rules affecting the acquisition, use, dissemination, and retention of the communications of U.S. persons appropriately balance the government’s valid interests with the privacy of U.S. persons.

This totality of the circumstances test is applicable when examining the implications of “incidental” collection. Where a wiretap is conducted in a criminal investigation pursuant to a warrant, satisfaction of the three requirements of the warrant clause (probable cause, particularity, and prior judicial review)⁴³⁴ renders the wiretap constitutionally reasonable — both as to the intended subjects of the surveillance *and* as to any persons who end up being incidentally overheard, the full range of whom the government can never predict.⁴³⁵ Likewise, under Title I of FISA, the government obtains warrant-like orders from the FISA court that require a modified form of particularity and probable cause.⁴³⁶ Just as the requirements of judicial review, probable cause, and particularity render a wiretap constitutionally reasonable in the criminal context, even as to individuals about whom the government had no prior evidence, so the corresponding protections of Title I of FISA render it reasonable under the Fourth Amendment, courts have held.⁴³⁷

However, where surveillance is undertaken without individual warrants or judicial orders, as under Section 702, and where the warrant requirements therefore are not satisfied, the legitimacy of the surveillance must be assessed under the reasonableness standard of the Fourth Amendment as described above, weighing the competing privacy

still have Fourth Amendment rights, but . . . what the FISA court has said is that the minimization procedures that are in place render that collection reasonable from a Fourth Amendment perspective.”); *see also* Government’s Unclassified Memorandum in Opposition to Defendants’ Motion to Suppress, at 62, *United States v. Muhtorov*, No. 12-0033 (D. Colo. May 9, 2014) (arguing that the Section 702 program’s targeting and minimization rules contribute to its reasonableness under the Fourth Amendment).

⁴³⁴ *Dalia v. United States*, 441 U.S. 238, 255 (1979) (listing the requirements of a search warrant).

⁴³⁵ *See United States v. Donovan*, 429 U.S. 413, 427 n.15 (1977); *United States v. Kahn*, 415 U.S. 143, 155 n.15 (1974); *United States v. Gaines*, 639 F.3d 423, 429-33 (8th Cir. 2011); *United States v. Urban*, 404 F.3d 754, 773-74 (3d Cir. 2005); *United States v. Tehfe*, 722 F.2d 1114, 1118 (3d Cir. 1983); *United States v. Ramsey*, 503 F.2d 524, 526 n.7 (7th Cir. 1974). Of course, even a validly authorized wiretap or other search can be executed in a constitutionally unreasonable manner.

⁴³⁶ *See In re Sealed Case*, 310 F.3d at 739-40.

⁴³⁷ *See, e.g., United States v. Stewart*, 590 F.3d 93, 129 (2d Cir. 2009); *In re Sealed Case*, 310 F.3d at 741; *United States v. Pelton*, 835 F.2d 1067, 1075 (4th Cir. 1987); *Cavanagh*, 807 F.2d at 789-91; *United States v. Duggan*, 743 F.2d 59, 79-80 & n.7 (2d Cir. 1984).

and governmental interests while taking into account the totality of circumstances. Thus, even where only foreigners outside the United States are targeted, the nature of the collection and use of some communications involving a U.S. person bears on the constitutional reasonableness of the program. Simply put, the “totality of the circumstances” that must be considered under the Fourth Amendment in this context may include factors such as why U.S. persons’ communications are acquired, the frequency with which they are acquired, how long they may be retained, who is given access to them, whether and how the government may query them for information about specific U.S. persons, under what circumstances they may be disseminated, and what degree of oversight attends to these matters. For instance, given the comparatively low standards for *collection* of information under Section 702, standards for querying the collected data to find the communications of specific U.S. persons may need to be more rigorous than where higher standards are required at the collection stage.

Applying this holistic inquiry to the Section 702 program therefore requires examining a web of factors bearing on the collection, use, dissemination, and retention of the communications of U.S. persons under the program. Pulling one of the threads of this web, in a more or less privacy-protective direction, alters the total picture. The ultimate Fourth Amendment assessment rests on an appraisal of the point at which any particular feature of the program, or any particular combination of features, goes too far and pushes the program across the threshold of unreasonableness.

In the Board’s view, the core of this 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 communicate foreign intelligence, using specific communications identifiers, subject to FISA court–approved targeting rules that have proven to be accurate in targeting persons outside the United States, and subject to multiple layers of rigorous oversight — fits within the totality of the circumstances test for reasonableness as it has been defined by the courts to date.

Outside of this fundamental core, certain aspects of the Section 702 program raise questions about whether its impact on U.S. persons pushes the program over the edge into constitutional unreasonableness. Such aspects include the scope of the incidental collection of U.S. persons’ communications, the use of “about” collection to acquire Internet communications that are neither to nor from the target of surveillance, the collection of MCTs that predictably will include U.S. persons’ Internet communications unrelated to the purpose of the surveillance, the use of database queries to search the information collected under the program for the communications of specific U.S. persons, and the possible use of

communications acquired under the program for criminal assessments, investigations, or proceedings that have no relationship to foreign intelligence.⁴³⁸

These features of the Section 702 program, and their cumulative potential effects on the privacy of U.S. persons, push the entire program close to the line of constitutional reasonableness. At the very least, too much expansion in the collection of U.S. persons' communications or the uses to which those communications are put may push the program over the line. The response if any feature tips the program over the line is not to discard the entire program; instead, it is to address that specific feature.

With these concerns in mind, the next section of this Report offers a set of proposals designed to push the program more comfortably into the sphere of reasonableness, ensuring that the program remains tied to its constitutionally legitimate core. Because the same factors that bear on Fourth Amendment reasonableness under a "totality of the circumstances" test are equally relevant to an assessment based purely on policy, the Board opts to present its proposals for changes to the Section 702 program as policy recommendations, without rendering a judgment about which, if any, of those proposals might be necessary from a constitutional perspective. This approach is fitting because some of the facts that may bear on the reasonableness of the Section 702 program under the Fourth Amendment, such as how many U.S. persons' communications and domestic communications are acquired, simply are not known. It also permits us to offer the recommendations that we believe are merited on privacy grounds without making fine-tuned determinations about whether any aspect of the status quo is constitutionally fatal, and without limiting our recommendations to changes that we may deem constitutionally required.

In sum, the Board has carefully considered the totality of the circumstances surrounding the Section 702 program that must be considered in assessing the program's reasonableness under the Fourth Amendment, but rather than render a judgment about the constitutionality of the program as a whole, the Board instead has addressed the areas of concern it has identified by formulating recommendations for changes to those aspects of the program.

⁴³⁸ Anecdotally, the FBI has advised the Board that it is extremely unlikely that an agent or analyst who is conducting an assessment of a non-national security crime would get a responsive result from the query against the Section 702-acquired data.

IV. Analysis of Treatment of Non-U.S. Persons

The treatment of non-U.S. persons under U.S. surveillance programs raises important but difficult legal and policy questions. Privacy is a human right that has been recognized most prominently in the International Covenant on Civil and Political Rights (“ICCPR”), an international treaty ratified by the U.S. Senate. Many of the generally applicable protections that already exist under U.S. surveillance laws apply to U.S. and non-U.S. persons alike. The President’s recent initiative under Presidential Policy Directive 28 on Signals Intelligence (“PPD-28”)⁴³⁹ will further address the extent to which non-U.S. persons should be afforded the same protections as U.S. persons under U.S. surveillance laws. Because PPD-28 invites the PCLOB to be involved in its implementation, the Board has concluded that it can make its most productive contribution in assessing these issues in the context of the PPD-28 review process.

A. Existing Legal Protections for Non-U.S. Persons’ Privacy

A number of provisions of Section 702, as well as provisions in other U.S. surveillance laws, protect the privacy of U.S. and non-U.S. persons alike. These protections can be found, for example, in (1) limitations on the scope of authorized surveillance under Section 702; (2) damages and other civil remedies that are available to subjects of unauthorized surveillance as well as sanctions that can be imposed on government employees who engage in such conduct; and (3) prohibitions on unauthorized 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-U.S. 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.⁴⁴⁰ 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 U.S. national defense or foreign affairs.⁴⁴¹ Further limitations are imposed by the required certifications identifying the specific categories of foreign intelligence information, which are reviewed and

⁴³⁹ Presidential Policy Directive — Signals Intelligence Activities, Policy Directive 28, 2014 WL 187435 (Jan. 17, 2014) (“PPD-28”), *available at* <http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>.

⁴⁴⁰ 50 U.S.C. § 1881a(a).

⁴⁴¹ 50 U.S.C. § 1801(e).

approved by the FISC.⁴⁴² These limitations do *not* permit unrestricted collection of information about foreigners.

The second group of statutory privacy protections for non-U.S. persons are the penalties that apply to government employees who engage in improper information collection practices — penalties that apply whether the victim is a U.S. person or a non-U.S. person. Thus, if an intelligence analyst were to use the Section 702 program improperly to acquire information about a non-U.S. 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.⁴⁴³ Finally, a non-U.S. 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.⁴⁴⁴ In sum, if a U.S. intelligence analyst were to use the Section 702 program to collect information about a non-U.S. person where it did not both meet the definition of foreign intelligence and relate to one of the certifications approved by the FISA court, he or she could face not only the loss of a job, but the prospect of a term of imprisonment and civil damage suits.

The third privacy protection covering non-U.S. persons is the statutory restriction on improper secondary use found at 50 U.S.C. § 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.”⁴⁴⁵ Congress included this language “to insure that information concerning foreign visitors and other non-U.S. persons . . . is not used for illegal purposes.”⁴⁴⁶ Thus, use of Section 702 collection for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion, would violate Section 1806.

Further, FISA provides special protections in connection with legal proceedings, under which an aggrieved person — a term that includes non-U.S. persons — is required to be notified prior to the disclosure or use of any Section 702–related information in any

⁴⁴² 50 U.S.C. § 1881a(g)(2)(A)(v).

⁴⁴³ See Bates October 2011 Opinion, *supra*, at 17 n.15, 2011 WL 10945618, at *6 n.15 (criminal penalties of 50 U.S.C. § 1809 of the FISA are implicated by Section 702 surveillance that strays beyond the scope of the court’s order approving such activities). In addition, to the extent that Section 702 program surveillance strayed from the certifications approved by the FISA court, it would potentially implicate the criminal provisions of the Wiretap Act, 18 U.S.C. § 2511(1), because the Section 702 surveillance would then lose its safe harbor for authorized FISA activities under Section 2511(2)(e) of the Wiretap Act.

⁴⁴⁴ See 50 U.S.C. § 1810 (“aggrieved person” not limited to U.S. persons); 18 U.S.C. § 2520 (“any person” not limited to U.S. persons); see also *Suzlon Energy Ltd. v. Microsoft Corp.*, 671 F.3d 726, 728-29 (9th Cir. 2011) (construing the statutory term “any person” to include non-U.S. persons).

⁴⁴⁵ 50 U.S.C. § 1806(a) (incorporated into Section 702 by 50 U.S.C. § 1881e(a)).

⁴⁴⁶ H.R. Rep. No. 95-1283(I), at 88-90 (1978) (discussing Section 106 of H.R. 7308, which became Section 106 of the FISA).

federal or state court.⁴⁴⁷ 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 authorizing Section 702 certification.⁴⁴⁸ Determinations regarding whether the Section 702 acquisition was lawful and authorized are made by a United States District Court, which has the authority to suppress any evidence that was unlawfully obtained or derived.⁴⁴⁹

Finally, as a practical matter, non-U.S. persons also benefit from the access and retention restrictions required by the different agencies' minimization and/or targeting procedures. While these procedures are legally required only for U.S. persons, the cost and difficulty of identifying and removing U.S. person information from a large body of data means that typically the entire dataset is handled in compliance with the higher U.S. person standards.

B. President's Initiative to Protect the Privacy of Non-U.S. Persons

As a matter of international law, privacy is a human right that has been recognized most prominently in the ICCPR, an international treaty ratified by the U.S. Senate. The question of how to apply the ICCPR right of privacy to national security surveillance, however, especially surveillance conducted in one country that may affect residents of another country, has to this point not been settled among the signatories to the treaty and is the subject of ongoing spirited debate.⁴⁵⁰

The executive branch is currently engaged in an extensive review of the extent to which, as a policy matter, the United States should afford all persons, regardless of nationality, a common baseline level of privacy protections in connection with foreign intelligence surveillance. This review began on January 17 of this year, when President Obama issued PPD-28,⁴⁵¹ in which he directed the review of the treatment of information regarding non-U.S. persons in connection with its surveillance programs.

Issues relating to the treatment of non-U.S. persons in government surveillance programs are by no means limited to the Section 702 program. Questions arise in

⁴⁴⁷ See 50 U.S.C. § 1806(c), (d).

⁴⁴⁸ 50 U.S.C. § 1806(e).

⁴⁴⁹ 50 U.S.C. § 1806(f), (g).

⁴⁵⁰ The United States currently interprets the ICCPR as not applying extra-territorially. Nonetheless the Board has received thoughtful comments and testimony arguing to the contrary. The Board also notes that in November 2013, the United Nations adopted, with United States support, a Resolution on "The right to privacy in the digital age." This resolution includes a provision requesting that the United Nations High Commissioner for Human Rights develop and present a report examining "the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or interception of digital communications and collection of personal data, including on a mass scale." This report is expected to be presented in August 2014.

⁴⁵¹ PPD-28, *supra*.

connection with signals intelligence conducted under other statutes and programs, including Executive Order 12333. Under PPD-28, the government has begun to address, as a matter of policy, the privacy and civil liberties of non-U.S. persons in connection with the full spectrum of signals intelligence programs conducted by the United States. The introduction to that directive notes 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.”⁴⁵² The government is presently in the process of implementing the principles set forth in that directive, including the requirement that “signals intelligence activities shall be as tailored as feasible.”⁴⁵³ PPD-28 sets forth a number of principles that have historically been, or will be, implemented, among them:

Privacy and civil liberties shall be integral considerations in the planning of U.S. signals intelligence activities. The United States shall not collect signals intelligence for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion. Signals intelligence shall be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions and not for any other purposes.⁴⁵⁴

Further, PPD-28 provides that:

U.S. 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.⁴⁵⁵

The Intelligence Community has already begun reviewing various options for implementing PPD-28, and the Board will engage in this process. PPD-28 specifically provides for direct PCLOB participation:

The Privacy and Civil Liberties Oversight Board is encouraged to provide [the President] with a report that assesses the implementation of any matters contained within this directive that fall within its mandate.⁴⁵⁶

⁴⁵² PPD-28, *supra*.

⁴⁵³ PPD-28, *supra*, § 3(d).

⁴⁵⁴ PPD-28, *supra*, § 3(b).

⁴⁵⁵ PPD-28, *supra*, § 4.

⁴⁵⁶ PPD-28, *supra*, § 5(b).

The Board has thus concluded that the optimal way for it to assess the treatment of information of non-U.S. persons is in the broader context of the PPD-28 review where it can evaluate other surveillance programs, along with Section 702, with a view to an integrated approach to foreign subjects of surveillance and the collection of signals intelligence. The implementation of PPD-28 may change the way Section 702 is operated and in so doing alleviate some of the concerns that have been voiced about its treatment of non-U.S. persons.

Part 5:
POLICY ANALYSIS

I. Introduction

In the Board's assessment, the Section 702 program has proven valuable in enabling the government to prevent acts of terrorism within the United States and abroad, and to pursue other foreign intelligence goals. The program has helped the government to learn about the membership and activities of terrorist organizations, as well as to discover previously unknown terrorist operatives and disrupt specific terrorist plots. Although the program is large in scope and involves collecting a great number of communications, it consists entirely of targeting individual persons and acquiring communications associated with those persons, from whom the government has reason to expect it will obtain certain types of foreign intelligence. The program does not operate by collecting communications in bulk.

At the same time, the communications of U.S. persons or people located in the United States may be acquired by the government under Section 702 in the course of targeting non-U.S. persons located abroad. The breadth of collection under the program and its technical complexity enhance this possibility. The communications of U.S. persons can be acquired when a U.S. person is in contact with a foreign target (who need not be involved in wrongdoing in order to be targeted), when the government makes a mistake, and in certain other situations. The government's ability to query its databases for the communications of specific U.S. persons, and to retain and disseminate such communications under certain circumstances, heightens the potential for privacy intrusions.

The Board has been impressed with the rigor of the government's efforts to ensure that it acquires only those communications it is authorized to collect, and that it targets only those persons it is authorized to target. Moreover, the government has taken seriously its obligations to establish and adhere to a detailed set of rules regarding how it handles U.S. person communications that it acquires under the program. Available figures suggest, consistent with the Board's own assessment, that the primary focus of the Section 702 program remains monitoring non-U.S. persons located overseas for valid foreign intelligence purposes. Nevertheless, there are some indications that the government may be gathering and utilizing a significant amount of information about U.S. persons under Section 702. While the Board has seen no evidence of abuse of this information for improper purposes, the collection and examination of personal communications can be a

privacy intrusion even in the absence of abuse, and a number of the Board's recommendations are motivated by a desire to provide more clarity and transparency regarding the government's activities in the Section 702 program.

II. Value of the Section 702 Program

A. Advantages and Unique Capabilities

The Section 702 program makes a substantial contribution to the government's efforts to learn about the membership, goals, and activities of international terrorist organizations, and to prevent acts of terrorism from coming to fruition. Section 702 allows the government to acquire a greater range of foreign intelligence than it otherwise would be able to obtain, and it provides a degree of flexibility not offered by comparable surveillance authorities.

Because the oversight mandate of the Board extends only to those measures taken to protect the nation from terrorism, our focus in this section is limited to the counterterrorism value of the Section 702 program, although the program serves a broader range of foreign intelligence purposes.⁴⁵⁷

Section 702 enables the government to acquire the contents of international telephone and Internet communications in pursuit of foreign intelligence. While this ability is to some degree provided by other legal authorities, particularly "traditional" FISA and Executive Order 12333, Section 702 offers advantages over these other authorities.

In order to conduct electronic surveillance under "traditional" FISA (i.e., Title I of the Foreign Intelligence Surveillance Act of 1978), the government must persuade the Foreign Intelligence Surveillance Court ("FISC" or "FISA court"), under a standard of probable cause, that an individual it seeks to target for surveillance is an agent of a foreign power, and that the telephone number or other communications facility it seeks to monitor is used, or is about to be used, by a foreign power or one of its agents.⁴⁵⁸ In addition, a high-level executive branch official must certify (with a supporting statement of facts) that a significant purpose of the surveillance is to obtain foreign intelligence, and that the information sought cannot reasonably be obtained through normal investigative techniques.⁴⁵⁹ To meet these requirements and satisfy the probable cause standard, facts must be gathered by the Intelligence Community, a detailed FISA court application must be drafted by the DOJ, the facts in the application must be vetted for accuracy, the senior

⁴⁵⁷ See page 25 of this Report.

⁴⁵⁸ 50 U.S.C. § 1805(a)(2).

⁴⁵⁹ 50 U.S.C. § 1804(a)(6).

government official's certification must be prepared, the Attorney General must approve the application, and the application must be submitted to the FISA court, which must review it, determine if the pertinent standards are met, and, if so, grant it.⁴⁶⁰ These steps consume significant time and resources.⁴⁶¹ In practice, FISA applications are lengthy and the process not infrequently takes weeks from beginning to final approval.⁴⁶²

This system is deliberately rigorous, for it was designed to provide a check on the government's surveillance of U.S. persons and other people located in the United States. Its goal was to prevent the abusive and politically motivated surveillance of U.S. persons and domestic activists that had occurred under the guise of foreign intelligence surveillance in the mid-twentieth century. Under FISA, electronic surveillance may be directed only at individuals who are acting at the behest of a foreign power (such as a foreign government or international terrorist organization), only for legitimate foreign intelligence purposes, and only where the aims of the surveillance cannot be achieved by other means.⁴⁶³ The statute's procedural hurdles help to ensure that surveillance takes place only after detailed analysis, a strong factual showing, measured judgment by high-level executive branch officials, and approval by a neutral judge.

Although the FISA process was designed for surveillance directed at people located in the United States, the government later sought and obtained approval from the FISA court to use this process to target foreign persons located outside the United States as well. Developments in communications technology and the Internet services industry meant that such surveillance could feasibly be conducted from within the United States in some instances.⁴⁶⁴ Utilizing the process of traditional FISA to target significant numbers of individuals overseas, however, required considerable time and resources, and government officials have argued that it slowed and sometimes prevented the acquisition of important intelligence.⁴⁶⁵

⁴⁶⁰ See 50 U.S.C. §§ 1804, 1805.

⁴⁶¹ These steps also must be repeated each time the government wishes to continue the surveillance beyond the time limit specified in the original order. See 50 U.S.C. § 1805(d).

⁴⁶² FISA permits surveillance to begin prior to court approval in emergency situations, but in order to exercise this option the Attorney General must make a determination that an emergency exists and that the factual basis required for the surveillance exists, and an application must be submitted to the FISA court for the normal probable cause determination within seven days. See 50 U.S.C. § 1805(e).

⁴⁶³ Moreover, when the target of surveillance is a U.S. person, that person must be "knowingly" acting on behalf of a foreign power. See 50 U.S.C. § 1801(b)(1), (2). An exception to the requirement that the target be acting on behalf of a foreign power permits a so-called "lone wolf" with no apparent connection to a foreign power to be targeted, if there is probable cause that the person is engaged in international terrorism or proliferation of weapons of mass destruction. See 50 U.S.C. §§ 1801(b)(1)(C), (D), 1805(a)(2)(A).

⁴⁶⁴ See pages 16-18 of this Report.

⁴⁶⁵ See pages 18-19 of this Report.

Section 702 imposes significantly fewer limits on the government when it targets non-U.S. persons located abroad, permitting greater flexibility and a dramatic increase in the number of people who can realistically be targeted.⁴⁶⁶ Rather than approving or denying individual targeting requests, the FISA court authorizes the surveillance program as a whole, approving the certification in which the government identifies the types of foreign intelligence information sought and the procedures the government uses to target people and handle the information it obtains.⁴⁶⁷ Targets of surveillance need not be agents of foreign powers; instead, the government may target any non-U.S. person overseas whom it reasonably believes has or is likely to communicate designated types of foreign intelligence.⁴⁶⁸ The government need not have probable cause for this belief, or for its belief that the target uses the particular selector, such as a telephone number or email address, to be monitored. There is no requirement that the information sought cannot be acquired through normal investigative techniques. Targeting decisions are made by NSA analysts and reviewed only within the executive branch.⁴⁶⁹ Once monitoring of a particular person begins, it may continue until new information indicates that the person no longer is an appropriate target. Whether a person remains a valid target must be reviewed annually.⁴⁷⁰

These differences allow the government to target a much wider range of foreigners than was possible under traditional FISA. For instance, people who might have knowledge about a suspected terrorist can be targeted even if those people are not themselves involved in terrorism or any illegitimate activity.

In addition to expanding the pool of potential surveillance targets, Section 702 also enables a much greater degree of flexibility, allowing the government to quickly begin monitoring new targets and communications facilities without the delay occasioned by the requirement to secure approval from the FISA court for each targeting decision.

As a result of these two factors, the number of people who can feasibly be targeted is significantly greater under Section 702 than under the traditional FISA process. And

⁴⁶⁶ Under FISA and the FISA Amendments Act, the term “United States person” includes U.S. citizens, legal permanent residents, unincorporated associations with a substantial number of U.S. citizens or legal permanent residents as members, and corporations incorporated in the United States. It does not include associations or corporations that qualify as a “foreign power.” See 50 U.S.C. § 1801(i).

⁴⁶⁷ 50 U.S.C. § 1881a(a), (i).

⁴⁶⁸ NSA DIRECTOR OF CIVIL LIBERTIES AND PRIVACY OFFICE REPORT: NSA’S IMPLEMENTATION OF FOREIGN INTELLIGENCE SURVEILLANCE ACT SECTION 702, at 4 (April 16, 2014) (“NSA DCLPO REPORT”), available at <http://www.dni.gov/files/documents/0421/702%20Unclassified%20Document.pdf>.

⁴⁶⁹ NSA DCLPO REPORT, *supra*, at 4-5.

⁴⁷⁰ Analysts are required to review the communications acquired from a target at least annually, to ensure that the targeting is still expected to provide the foreign intelligence sought and that the person otherwise remains an appropriate target under Section 702. See NSA DCLPO REPORT, *supra*, at 6.

indeed, the number of targets under the program has been steadily increasing since the statute was enacted in 2008.

The government also conducts foreign intelligence surveillance outside of the United States against non-U.S. persons under the authority of Executive Order 12333. In some instances, this surveillance can capture the same communications that the government obtains within the United States through Section 702. And because this collection takes place outside the United States, it is not restricted by the detailed rules of FISA outlined above.⁴⁷¹ Nevertheless, Section 702 offers advantages over Executive Order 12333 with respect to electronic surveillance. The fact that Section 702 collection occurs in the United States, with the compelled assistance of electronic communications service providers, contributes to the safety and security of the collection, enabling the government to protect its methods and technology. In addition, acquiring communications with the compelled assistance of U.S. companies allows service providers and the government to manage the manner in which the collection occurs. By helping to prevent incidents of overcollection and swiftly remedy problems that do occur, this arrangement can benefit the privacy of people whose communications are at risk of being acquired mistakenly.

B. Contributions to Counterterrorism

The Section 702 program has proven valuable in a number of ways to the government's efforts to combat terrorism. It has helped the United States learn more about the membership, leadership structure, priorities, tactics, and plans of international terrorist organizations. It has enabled the discovery of previously unknown terrorist operatives as well as the locations and movements of suspects already known to the government. It has led to the discovery of previously unknown terrorist plots directed against the United States and foreign countries, enabling the disruption of those plots.

While the Section 702 program is indeed a *program*, operating to some degree as a cohesive whole and approved by the FISA court accordingly, its implementation consists entirely of targeting specific individuals about whom the government already knows something. Because surveillance is conducted on an individualized basis where there is reason to target a particular person, it is perhaps unsurprising that the program yields a great deal of useful information.

The value of the Section 702 program is to some extent reflected in the breadth of NSA intelligence reporting based on information derived from the program. Since 2008, the number of signals intelligence reports based in whole or in part on Section 702 has

⁴⁷¹ FISA does not generally cover surveillance conducted outside the United States, except where the surveillance intentionally targets a particular, known U.S. person, or where it acquires radio communications in which the sender and all intended recipients are located in the United States and the acquisition would require a warrant for law enforcement purposes. *See* 50 U.S.C. §§ 1801(f), 1881c.

increased exponentially. A significant portion of those reports relate to counterterrorism, and the NSA disseminates hundreds of reports per month concerning terrorism that include information derived from Section 702. Presently, over a quarter of the NSA's reports concerning international terrorism include information based in whole or in part on Section 702 collection, and this percentage has increased every year since the statute was enacted. These reports are used by the recipient agencies and departments for a variety of purposes, including to inform senior leaders in government and for operational planning.

More concretely, information acquired from Section 702 has helped the Intelligence Community to understand the structure and hierarchy of international terrorist networks, as well as their intentions and tactics. In even the most well-known terrorist organizations, only a small number of individuals have a public presence. Terrorist groups use a number of practices to obscure their membership and activities. Section 702 has enabled the U.S. government to monitor these terrorist networks in order to learn how they operate and to understand how their priorities, strategies, and tactics continue to evolve.

Monitoring these networks under Section 702 has led the government to identify previously unknown individuals who are involved in international terrorism. Identifying such persons allows the government to pursue new efforts focusing on those individuals and the disruption of their activities, such as taking action to prevent them from entering the United States. Finally, the flexibility of Section 702 surveillance enables the government to effectively maintain coverage on particular individuals as they add or switch their modes of communications.

As important as discovering the identities of individuals engaged in international terrorism is determining where those individuals are located. Modern communications permit the members of a terrorist group, and even a small number of people involved in a specific plot, to be spread out all over the world. Information acquired from Section 702 has been used to monitor individuals believed to be engaged in terrorism.

In one case, for example, the NSA was conducting surveillance under Section 702 of an email address used by an extremist based in Yemen. Through that surveillance, the agency discovered a connection between that extremist and an unknown person in Kansas City, Missouri. The NSA passed this information to the FBI, which identified the unknown person, Khalid Ouazzani, and subsequently discovered that he had connections to U.S.-based Al Qaeda associates, who had previously been part of an abandoned early stage plot to bomb the New York Stock Exchange. All of these individuals eventually pled guilty to providing and attempting to provide material support to Al Qaeda.

Finally, pursuit of the foregoing information under Section 702 has led to the discovery of previously unknown terrorist plots and has enabled the government to

disrupt them. By providing the sites of specific targets of attacks, the means being contemplated to carry out the attacks, and the identities and locations of the participants, the Section 702 program has directly enabled the thwarting of specific terrorist attacks, aimed at the United States and at other countries.

For instance, in September 2009, the NSA monitored under Section 702 the email address of an Al Qaeda courier based in Pakistan. Through that collection, the agency intercepted emails sent to that address from an unknown individual located in the United States. Despite using language designed to mask their true intent, the messages indicated that the sender was urgently seeking advice on the correct mixture of ingredients to use for making explosives. The NSA passed this information to the FBI, which used a national security letter to identify the unknown individual as Najibullah Zazi, located near Denver, Colorado. The FBI then began intense monitoring of Zazi, including physical surveillance and obtaining legal authority to monitor his Internet activity. The Bureau was able to track Zazi as he left Colorado a few days later to drive to New York City, where he and a group of confederates were planning to detonate explosives on subway lines in Manhattan within the week. Once Zazi became aware that law enforcement was tracking him, he returned to Colorado, where he was arrested soon after. Further investigative work identified Zazi's co-conspirators and located bomb-making components related to the planned attack. Zazi and one of his confederates later pled guilty and cooperated with the government, while another confederate was convicted and sentenced to life imprisonment. Without the initial tip-off about Zazi and his plans, which came about by monitoring an overseas foreigner under Section 702, the subway-bombing plot might have succeeded.

In cases like the Zazi and Ouazzani investigations, one might ask whether the government could have monitored the communications of the overseas extremists without Section 702, using the traditional FISA process. In some instances, that might be the case. But the process of obtaining court approval for the surveillance under the standards of traditional FISA may, for the reasons explained above, limit the number of people the government can feasibly target and increase the delay before surveillance on a target begins, such that significant communications could be missed.

The Board has received information about other instances in which the Section 702 program has played a role in counterterrorism efforts. Most of these instances are included in a compilation of 54 "success stories" involving the Section 215 and 702 programs that was prepared by the Intelligence Community last year in the wake of Edward Snowden's unauthorized disclosures. Other examples have been shared with the Board more recently. Information about these cases has not been declassified, but some general information about them can be shared. In approximately twenty cases that we have reviewed, surveillance conducted under Section 702 was used in support of an already existing counterterrorism investigation, while in approximately thirty cases, Section 702

information was the initial catalyst that identified previously unknown terrorist operatives and/or plots. In the vast majority of these cases, efforts undertaken with the support of Section 702 appear to have begun with narrowly focused surveillance of a specific individual whom the government had a reasonable basis to believe was involved with terrorist activities, leading to the discovery of a specific plot, after which a short, intensive period of further investigation ensued, leading to the identification of confederates and arrests of the plotters. A rough count of these cases identifies well over one hundred arrests on terrorism-related offenses. In other cases that did not lead to disruption of a plot or apprehension of conspirators, Section 702 appears to have been used to provide warnings about a continuing threat or to assist in investigations that remain ongoing. Approximately fifteen of the cases we reviewed involved some connection to the United States, such as the site of a planned attack or the location of operatives, while approximately forty cases exclusively involved operatives and plots in foreign countries.⁴⁷²

C. Contributions to Other Foreign Intelligence Efforts

As noted above, the oversight mandate of our Board extends only to those measures taken by the government to protect the nation from terrorism. Some governmental activities, including the Section 702 program, are not aimed exclusively at preventing terrorism but also serve other foreign intelligence and foreign policy goals. The Section 702 program, for instance, is also used for surveillance aimed at countering the efforts of proliferators of weapons of mass destruction.⁴⁷³ Given that these other foreign intelligence purposes of the program are not strictly within the Board's mandate, we have not scrutinized the effectiveness of Section 702 in contributing to those other purposes with the same rigor that we have applied in assessing the program's contribution to counterterrorism. Nevertheless, we have come to learn how the program is used for these other purposes, including, for example, specific ways in which it has been used to combat weapons proliferation and the degree to which the program supports the government's efforts to gather foreign intelligence for the benefit of policymakers. Our assessment is that the program is highly valuable for these other purposes, in addition to its usefulness in supporting efforts to prevent terrorism.

⁴⁷² The examples described in this paragraph do not represent an exhaustive list of all instances in which the Section 702 program has proven useful, even in counterterrorism efforts.

⁴⁷³ See S. Rep. No. 112-229, at 32 (2012) (appendix reproducing Background Paper on Title VII of FISA Prepared by the Department of Justice and the Office of the Director of National Intelligence) ("Section 702 . . . lets us collect information about the intentions and capabilities of weapons proliferators and other foreign adversaries who threaten the United States.").

III. Privacy and Civil Liberties Implications of the Section 702 Program

A. Nature of the Collection under Section 702

1. Programmatic Surveillance

Unlike the telephone records program conducted by the NSA under Section 215 of the USA PATRIOT Act, the Section 702 program is not based on the indiscriminate collection of information in bulk. Instead, the program consists entirely of targeting specific persons about whom an individualized 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.⁴⁷⁴

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 and the ODNI (“the DOJ/ODNI oversight team”) in an effort to ensure that the person targeted is reasonably believed to be a non-U.S. 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.

Although the “persons” who may be targeted under Section 702 include corporations, associations, and entities as well as individuals,⁴⁷⁵ the government is not exploiting any legal ambiguity by “targeting” an entity like a major international terrorist organization and then engaging in indiscriminate or bulk collection of communications in order to later identify a smaller subset of communications that pertain to the targeted entity. To put it another way, the government is not collecting wide swaths of communications and then combing through them for those that are relevant to terrorism or contain other foreign intelligence. Rather, the government first identifies a communications identifier, like an email address, that it reasonably believes is used by the target, whether that target is an individual or an entity. It then acquires only those communications that are related to this identifier.⁴⁷⁶ In other words, selectors are always

⁴⁷⁴ See pages 20-23 and 32-33 of this Report.

⁴⁷⁵ See 50 U.S.C. §§ 1801(m), 1881a(a).

⁴⁷⁶ The NSA’s “upstream collection” (described elsewhere in this Report) may require access to a larger body of international communications than those that contain a tasked selector. Nevertheless, the government has no ability to examine or otherwise make use of this larger body of communications, except to promptly determine whether any of them contain a tasked selector. Only those communications (or more precisely, “transactions”) that contain a tasked selector go into government databases. See pages 36-41 of this Report.

unique communications identifiers used by the targeted persons. So under the Section 702 program, the government cannot, for instance, acquire communications because they are associated with a particular region where the government believes it is likely to find information related to one of its targets. Collection is instead limited to the communications identifiers of the targets themselves.

Likewise, although the selectors that the government could use are not limited to telephone numbers and email addresses, the government is not creatively interpreting the meaning of “selectors” to engage in bulk collection under Section 702. Even in the complex realm of Internet communications, a selector always must be associated with a specific person or entity. Thus, acquisition is always based on selecting communications that are associated with the target.⁴⁷⁷

2. Contents of Private Telephone and Internet Communications

Under Section 702, the government acquires the *contents* of international communications — collecting Internet communications like emails and recording telephone calls — as well as the addressing information or “metadata” associated with those communications. The contents of such communications may be highly personal and sensitive. U.S. persons and people located in the United States may not be targeted under Section 702, but their communications nevertheless can be acquired, including when they are in contact with a foreigner located abroad who has been targeted. Thus, the chance of government intrusion into private matters may be comparatively higher for individuals who maintain frequent contact with family members, friends, acquaintances, or professional contacts outside of the United States.

After being acquired by the government, communications obtained through Section 702 are stored in databases for default periods of time.⁴⁷⁸ There, they are subject to being examined by NSA, CIA, and FBI analysts or agents in pursuit of foreign intelligence or evidence of a crime. Subject to the separate minimization procedures at each agency, communications can be identified and retrieved from these databases for examination based on their addressing information (such as the telephone numbers or email addresses involved), while Internet communications are also retrievable by scanning their contents for the presence of certain words or terms.

3. Scope of Targeting and Collection

While the Section 702 program is based entirely on individual targeting decisions, it nevertheless results in an extremely large amount of collection. In part, this is because

⁴⁷⁷ This is true even in the unique contexts of so-called “about” collection and “MCT” collection, both of which are discussed below.

⁴⁷⁸ See page 60 of this Report.

modern technology, especially the ability to store huge amounts of data, makes it logistically feasible to target large numbers of people. The breadth of collection is also possible because, as explained above, the standards under which targeting is permitted under Section 702 are less rigorous than those governing other surveillance activities conducted within the United States. The government enjoys much more latitude when targeting foreigners located outside the United States under Section 702 than it does when targeting people located in the United States under other legal authorities, even for foreign intelligence purposes. The range of people whom the government may target and the permissible reasons for that targeting are much broader, while the level of suspicion required and the legal steps the government must take before initiating surveillance are much lower. In particular, the FISA court approves the government's targeting and minimization procedures but plays no role in reviewing individual targeting decisions.⁴⁷⁹

As a result, the number of people targeted under Section 702 is considerable and collection has steadily grown. During the year 2013, 89,138 persons were targeted for collection under Section 702.

Thus, while the Board does not regard Section 702 as a "bulk" collection program, because it is based entirely on targeting the communications identifiers of specific people, neither does the program resemble traditional domestic surveillance conducted pursuant to individualized court orders based on probable cause. The FISA court instead determines whether to approve the surveillance program as a whole and plays a role in overseeing whether it stays within statutory and constitutional limits. The Section 702 program, in short, is perhaps best characterized by the term "programmatically surveillance."⁴⁸⁰

B. Acquisition of the Communications of U.S. Persons under Section 702

While the scope of targeting under Section 702 is broad, that targeting cannot include U.S. persons or people located in the United States. As a result, this program does not allow the government to gain comprehensive access to any U.S. person's communications: the government will not be able to hear every telephone call a U.S. person makes, for instance, or collect every email sent or received by that person. Instead, absent mistake or abuse, Section 702 enables the government to obtain only those communications that occur where a U.S. person is in contact with a targeted overseas foreigner, as well as those that are acquired in the unique circumstances of "about" and "MCT" collection (discussed below).

⁴⁷⁹ See pages 26-31 of this Report.

⁴⁸⁰ The Section 215 program, in contrast, represents both a bulk collection program and an example of programmatically surveillance.

Because it disallows *comprehensive* monitoring of any U.S. person, and prohibits deliberately acquiring even a single communication that is known to be solely among people located within the United States, the program would serve as a relatively poor vehicle to repress domestic dissent, monitor American political activists, or engage in other politically motivated abuses of the sort that came to light in the 1970s and prompted the enactment of FISA.

Nevertheless, as described below, under certain circumstances the program permits the government to collect a communication where one party is a U.S. person, including communications that are sensitive and private, and where the U.S. person may have taken steps to preserve the confidentiality of the communication. There are four main ways in which the Section 702 program, notwithstanding its focus on targeting foreigners located abroad, can lead to the acquisition of U.S. persons' communications.

1. Incidental Collection

A person targeted for surveillance who speaks on the phone or communicates over the Internet is communicating with someone else. That other person's communications with the target are said to have been "incidentally" acquired. In the context of the Section 702 program, the term "incidental collection" is used to refer to situations in which U.S. persons or people located in the United States have their communications acquired because they were in contact with a targeted foreigner located overseas. While the government cannot target U.S. persons or people located in the United States, it is permitted to acquire and in some cases retain and use communications in which a U.S. person is in contact with a target.

The term "incidental" is appropriate because such collection is not accidental or inadvertent, but rather is an anticipated collateral result of monitoring an overseas target.⁴⁸¹ But the term should not be understood to suggest that such collection is infrequent or that it is an inconsequential part of the Section 702 program.

The number of communications collected under Section 702 to which one party is a U.S. person or located in the United States is not known. And one of the purposes of the program is to discover communications between a target overseas and a person in the United States. Executive and legislative branch officials have repeatedly emphasized to us that, with respect to terrorism, communications involving someone in the United States are

⁴⁸¹ See Privacy and Civil Liberties Oversight Board, Transcript of Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, at 97 (Mar. 19, 2014) (statement of Robert Litt, General Counsel, ODNI), *available at* http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/19-March-2014_Public_Hearing_Transcript.pdf.

some of the “most important” communications acquired under the program.⁴⁸² And indeed, where the program has directly led to the discovery and disruption of terrorist plots, it has sometimes done so by helping to discover previously unknown operatives in the United States through their communications with terrorism suspects located abroad.⁴⁸³

From a privacy perspective, however, incidental collection under Section 702 differs in at least two significant ways from incidental collection that occurs in the course of a criminal wiretap or the traditional FISA process.

First, in the criminal or FISA context the targets of surveillance must be believed to be criminals or agents of a foreign power.⁴⁸⁴ That means that innocent U.S. persons need not worry about the government listening to their phone conversations or reading their emails except to the extent that they are communicating with suspected criminals or agents of foreign powers. The range of people whom the government may target under Section 702, on the other hand, is much broader. It is not limited to suspected terrorists or others engaged in nefarious activities. Instead, under an approved certification, the government may target any overseas foreigner who has or is likely to communicate certain kinds of foreign intelligence — who, for instance, may possess information “with respect to a foreign power or foreign territory that relates to . . . the conduct of the foreign affairs of the United States.”⁴⁸⁵ That person need not be acting at the behest of a foreign power or be engaged in any activities that are hostile toward the United States or would violate any laws. For instance, someone who has information about a terrorist operative may be targeted under Section 702, even if that person has no involvement in terrorism.

Second, to engage in traditional FISA or criminal electronic surveillance, the government must obtain approval from a judge, who independently assesses the legitimacy of the targeting and must be persuaded that the government’s beliefs about the person

⁴⁸² See Privacy and Civil Liberties Oversight Board, Transcript of Public Workshop regarding surveillance programs operated pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act, at 109 (July 9, 2013) (statement of Steven Bradbury, formerly DOJ Office of Legal Counsel) (stating that Section 702 “is particularly focused on communications in and out of the United States because . . . those are the most important communications you want to know about if you’re talking about a foreign terrorist suspect communicating to somebody you don’t know inside the United States”); see *id.* at 116 (statement of Kenneth Wainstein, formerly DOJ National Security Division/White House Homeland Security Advisor) (agreeing), available at <http://www.pclomb.gov/SiteAssets/9-july-2013/Public%20Workshop%20-%20Full.pdf>; see also *FISA for the 21st Century: Hearing before the Senate Comm. on the Judiciary*, 109th Cong. 9 (2006) (statement of General Michael V. Hayden, Director, CIA).

⁴⁸³ See pages 107-110 of this Report.

⁴⁸⁴ See 50 U.S.C. § 1805(a)(2)(A); 18 U.S.C. § 2518(3)(a).

⁴⁸⁵ 50 U.S.C. § 1801(e)(2)(B). The range of foreign intelligence that the government may seek under Section 702 is limited by the certifications approved by the FISA court. See pages 24-31 of this Report for a description of the certification process.

and/or communications facility being targeted are supported by probable cause.⁴⁸⁶ By providing a neutral check on the government's authority to conduct electronic surveillance, these protections help assure innocent U.S. persons that their conversations will not be incidentally acquired in the course of improper surveillance directed at another person.

These restrictions and checks are absent under Section 702. To be clear, such absence does not mean that the government has free rein: targeting rules, a system of intra- and inter-agency oversight, programmatic supervision by the FISA court, and a host of reporting requirements all work to ensure that the government's decisions about whom to monitor stay within legal bounds. But the expansiveness of the governing rules, combined with the technological capacity to acquire and store great quantities of data, permit the government to target large numbers of people around the world and acquire a vast number of communications. By 2011, for instance, the government was annually acquiring over 250 million Internet communications, in addition to telephone conversations.⁴⁸⁷ The current number is significantly higher. Even if U.S. persons' communications make up only a small percentage of this total, the absolute number of their communications acquired could be considerable.

Minimization requirements to some degree compensate for the possibility of broad incidental collection. Those rules are described in detail earlier in this Report,⁴⁸⁸ and their significance is discussed below. While the existence of minimization rules may temper the privacy impact of incidental collection, the scope of that collection may also bear on whether the minimization rules are adequate. The present lack of knowledge about the range of incidental collection under Section 702 therefore hampers attempts to gauge whether the program appropriately balances national security interests with the privacy of U.S. persons.

2. Inadvertent Collection

Sometimes the NSA acquires communications under Section 702 of U.S. persons or people located in the United States by mistake. This can occur when the NSA erroneously believes that a potential target is a foreigner or located outside the United States, and discovers the truth only after collection on that person begins. It can also occur as a result of human error, such as mistyping an email address in the targeting process. Additionally, mistakes can occur as a result of technological malfunctions. Finally, targets who were located outside the United States may travel into the country, making them no longer

⁴⁸⁶ See 50 U.S.C. § 1805; 18 U.S.C. § 2518.

⁴⁸⁷ Opinion at 29, [*Caption Redacted*], [Docket No. Redacted], 2011 WL 10945618, at *9 (FISA Ct. Oct. 3, 2011) (“Bates October 2011 Opinion”), available at <http://icontherecord.tumblr.com> (noting submitted affidavits by the Director or Acting Director of NSA and the Director of FBI).

⁴⁸⁸ See pages 50-66 of this Report.

eligible for targeting, before the NSA discovers this fact. While all of these possibilities create risks that the NSA will acquire communications that it is not authorized to collect, the Board has been impressed by the seriousness with which the government attempts to ensure that this does not occur.

In any surveillance program as large in scope as the Section 702 program, particularly where collection involves highly sophisticated technology, mistakes are inevitable. The Board believes that the Section 702 program is implemented in a manner that reasonably avoids such errors. Furthermore, experience has shown that where there have been more significant mistakes, the government discovers them and complies with the reporting requirements that demand prompt disclosure of compliance incidents to the FISA court and to the oversight committees in Congress.

There have been a few significant large-scale implementation problems in the Section 702 program, all revolving around technological matters. As described earlier, technical problems have in some instances led the government to acquire communications not authorized for collection under the program. More recently, the checks that are designed to provide indications that a target is located inside the United States were substantially non-functioning for over a year. In yet another incident, the NSA discovered that its systems for purging data were not operating completely, leading to the retention of information that should have been destroyed.⁴⁸⁹ In consultation with the FISA court, the government has resolved those issues appropriately and has worked to remedy the errors that were discovered.

Inadvertent collection can also occur on an individualized basis, such as where the NSA targets people whom it mistakenly believes are foreigners or located outside the United States. Commentators have questioned the rigor of the agency's "foreignness" determinations, particularly whether they rely on certain default assumptions where information about a person is lacking. The notion also has arisen that the agency employs a "51% test" in assessing the location and nationality of a potential target — in other words, that analysts need only be slightly more than half confident that the person being targeted is a non-U.S. person located outside the United States.

These characterizations are not accurate. In keeping with representations the government has made to the FISA court, NSA analysts consult multiple sources of information in attempting to determine a proposed target's foreignness, and they are obligated to exercise a standard of due diligence in that effort, making their determinations based on the totality of the circumstances. They also must document the information on

⁴⁸⁹ See page 79 of this Report.

which they based their assessments, which must be reviewed and approved by two senior analysts prior to targeting, and which are subject to further review later.⁴⁹⁰

Available figures suggest that the percentage of instances in which the NSA accidentally targets a U.S. person or someone in the United States is tiny. In 2013, the DOJ reviewed one year of data to determine the percentage of cases in which the NSA's targeting decisions resulted in the "tasking" of a communications identifier that was used by someone in the United States or was a U.S. person. The NSA's error rate, according to this review, was 0.4 percent.⁴⁹¹ Moreover, once a targeting decision has been made, that is not the end of the story. Soon after collection on a selector begins, analysts must review a sample of the communications that have recently been collected, to ensure that the email address or other selector actually is associated with the person whom the NSA intended to target, and that this person is a foreigner located outside the United States. Additional measures are employed to re-verify the validity of continued collection against the selector.⁴⁹² In addition, the DOJ/ODNI oversight team reviews every targeting decision, including the documentation on which the "foreignness" determination was made. The oversight team conducts on-site reviews as part of this process, and when the documentation available is not sufficient to demonstrate the basis of a foreignness determination, the oversight team requests and obtains additional information.⁴⁹³ The NSA counts the number of instances in which it discovers that a selector is or may be being used by someone in the United States — either because the target traveled to the United States or because the original targeting decision was erroneous. The percentage of such instances is also very small, with the total annual number of instances representing less than 1.5 percent of the average number of selectors targeted at any given moment.

To date, the DOJ/ODNI oversight team has not discovered any instances in which an analyst intentionally violated the statute, targeting procedures, or minimization procedures. In the history of the program, the government has identified only two instances of "reverse targeting" — that is, the prohibited targeting of overseas foreigners for the purpose of acquiring the communications of persons in the United States with whom they are in contact.⁴⁹⁴

⁴⁹⁰ NSA DCLPO REPORT, *supra*, at 4-5.

⁴⁹¹ See pages 71-72 of this Report.

⁴⁹² See pages 48-49 of this Report; NSA DCLPO REPORT, *supra*, at 6.

⁴⁹³ NSA DCLPO REPORT, *supra*, at 10.

⁴⁹⁴ See page 79 of this Report. In one case, the targeting resulted in no collection of communications. In the other case, all of the collection was purged.

In sum, as noted above, the Board is impressed by the rigor with which the government attempts to ensure that the persons it targets under Section 702 truly are non-U.S. persons located outside the United States.⁴⁹⁵

3. “About” Collection

One of the most controversial aspects of the Section 702 program is the practice of so-called “about” collection. This term describes the NSA’s acquisition of Internet communications that are neither to nor from an email address — but that instead merely include a reference to that selector.⁴⁹⁶ For instance, a communication between two third parties might be acquired because it contains a targeted email address in the body of the communication.⁴⁹⁷

The fact that the NSA acquires certain communications based on what is contained within the body of the communication has apparently led some to believe that the government is scanning the contents of U.S. persons’ international communications to see if they are discussing particular subjects or using particular key words. Initial news articles describing “about” collection may have contributed to this perception, reporting that the NSA “is searching the contents of vast amounts of Americans’ email and text communications into and out of the country, hunting for people who mention information about foreigners under surveillance[.]”⁴⁹⁸ This belief represents a misunderstanding of a more complex reality. “About” collection takes place exclusively in the NSA’s acquisition of Internet communications through its upstream collection process. That is the process whereby the NSA acquires communications as they transit the Internet “backbone” within the United States. This process is distinguished from the NSA’s PRISM collection, in which U.S.-based Internet service providers transmit communications to the government

⁴⁹⁵ See below for a discussion of what happens when the NSA discovers that it inadvertently acquired the communications of a U.S. person or someone in the United States.

⁴⁹⁶ See PCLOB March 2014 Hearing Transcript, *supra*, at 13 (statement of Rajesh De, General Counsel, NSA).

⁴⁹⁷ See The Intelligence Community’s Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, at 4 (2012) (describing differences between targeting individuals under traditional FISA electronic surveillance provisions and targeting pursuant to Section 702). This document accompanied a 2012 letter sent by the Department of Justice and the Office of the Director of National Intelligence to the Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence urging the reauthorization of Section 702. See Letter from Kathleen Turner, Director of Legislative Affairs, ODNI, and Ronald Weich, Assistant Attorney General, Office of Legislative Affairs, DOJ to the Hon. Dianne Feinstein, Chairman, Senate Committee on Intelligence, et. al. (May 4, 2012), *available at* http://www.dni.gov/files/documents/Ltr%20to%20HPSCI%20Chairman%20Rogers%20and%20Ranking%20Member%20Ruppersberger_Scan.pdf.

⁴⁹⁸ Charlie Savage, *N.S.A. Said to Search Content of Messages to and From U.S.*, N.Y. TIMES (Aug. 8, 2013).

directly.⁴⁹⁹ Whereas PRISM collection is a comparatively simple process, because the government obtains communications of a service provider's customers directly from that provider, the upstream process is more complex, depending upon the use of collection devices with technological limitations that significantly affect the scope of collection.⁵⁰⁰ Because of the way that Internet communications are transmitted in the form of data packets, the NSA's collection devices acquire what the agency and the FISA court have termed Internet "transactions."⁵⁰¹ As a result of this acquisition technique, the FISA court has explained, "the NSA's upstream collection devices acquire any Internet transaction transiting the device if the transaction contains a targeted selector anywhere within it[.]"⁵⁰²

This means that an Internet communication between third parties, not involving the target, can be acquired by the NSA if it contains a reference, for instance, to the email address of a target.⁵⁰³ For this reason, "about" collection raises at least two serious concerns, one relatively simple, the other more complex.

First, "about" collection may be more likely than other forms of collection to acquire wholly domestic communications — something not authorized by Section 702. Because "about" communications are not to or from the email address that was tasked for acquisition,⁵⁰⁴ which is used by a person reasonably believed to be located outside the United States, there is no guarantee that any of the participants to the communication are located outside the United States. In part to compensate for this problem, the NSA takes additional measures with its upstream collection to ensure that no communications are acquired that are entirely between people located in the United States. These measures can include, for instance, employing Internet protocol filters to acquire only communications that appear to have at least one end outside the United States.⁵⁰⁵ In this process, Internet communications are first filtered to eliminate potential domestic communications, and then are screened to capture only communications containing a tasked selector.

⁴⁹⁹ The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3-4; NSA DCLPO REPORT, *supra*, at 5. See pages 33-34 of this Report.

⁵⁰⁰ Bates October 2011 Opinion, *supra*, at 30, 2011 WL 10945618, at *10.

⁵⁰¹ Bates October 2011 Opinion, *supra*, at 30, 2011 WL 10945618, at *10.

⁵⁰² Bates October 2011 Opinion, *supra*, at 31, 2011 WL 10945618, at *11.

⁵⁰³ Joint Statement of Lisa O. Monaco, Assistant Attorney General, National Security Division, Dept. of Justice, et. al., *Hearing Before the House Permanent Select Comm. on Intelligence: FISA Amendments Act Reauthorization*, at 7 (Dec. 8, 2011) ("December 2011 Joint Statement"), available at <http://www.dni.gov/files/documents/Joint%20Statement%20FAA%20Reauthorization%20Hearing%20-%20December%202011.pdf>.

⁵⁰⁴ As explained earlier, persons are *targeted* under Section 702 while the selectors used by those persons are *tasked*.

⁵⁰⁵ NSA DCLPO REPORT, *supra*, at 5-6.

While we believe that the measures taken by the NSA to exclude wholly domestic “about” communications may be reasonable in light of current technological limits, they are not perfect.⁵⁰⁶ Even where both parties to a communication are located in the United States, in a number of situations the communication might be routed internationally, in which case it could be acquired by the NSA’s upstream collection devices.⁵⁰⁷ There are reasons to suppose that this occurs rarely, but presently no one knows how many wholly domestic communications the NSA may be acquiring each year as a result of “about” collection.⁵⁰⁸

The more fundamental concern raised by “about” collection is that it permits the government to acquire communications exclusively between people about whom the government had no prior suspicion, or even knowledge of their existence, based entirely on what is contained within the contents of their communications.⁵⁰⁹ This practice fundamentally differs from “incidental” collection, discussed above. While incidental collection also permits the government to acquire communications of people about whom it may have had no prior knowledge, that is an inevitable result of the fact that conversations generally involve at least two people: acquiring a target’s communications by definition involves acquiring his communications with other people. But no effort is made to acquire those other peoples’ communications — the government simply is acquiring the target’s communications. In “about” collection, by contrast, the NSA’s

⁵⁰⁶ December 2011 Joint Statement, *supra*, at 7 (acknowledging that the NSA’s efforts “are not perfect”).

⁵⁰⁷ *See generally* Bates October 2011 Opinion, *supra*, at 34, 2011 WL 10945618, at *11.

⁵⁰⁸ Although the NSA conducted a study in 2011, at the behest of the FISA court, to estimate how many wholly domestic communications it was annually acquiring as a result of collecting “MCTs” (discussed below), the study did not focus on how many domestic communications the NSA may be acquiring due to “about” collection where the communication acquired was not an MCT but rather a single, discrete communication. Bates October 2011 Opinion, *supra*, at 34 n.32, 2011 WL 10945618, at *11, n.32. At the urging of the FISA court, the NSA subsequently spent some time examining this question, but ultimately did not provide an estimate, instead explaining to the court the logistical reasons that the chance of acquiring domestic communications in “about” collection “should be smaller — and certainly no greater — than potentially encountering wholly domestic communications within MCTs.” *Id.* This statement prompted the FISA court to adopt the assumption that the percentage of wholly domestic communications within the agency’s “about” collection might equal the percentage of wholly domestic communications within its collection of “MCTs,” leading to an estimate of as many as 46,000 wholly domestic “about” communications acquired each year. *Id.* We do not view this as a particularly valid estimate, because there is no reason to suppose that the number of wholly domestic “about” communications matches the number of wholly domestic MCTs, but the fact remains that the NSA cannot say how many domestic “about” communications it may be obtaining each year.

⁵⁰⁹ *See* December 2011 Joint Statement, *supra*, at 7 (“[U]pstream collection allows NSA to acquire, among other things, communications about a target where the target is not itself a communicant.”); The Intelligence Community’s Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 4 (“Upstream collection . . . lets NSA collect electronic communications that contain the targeted e-mail address in the body of a communication between two third parties.”).

collection devices can acquire communications to which the target is not a participant, based at times on their contents.⁵¹⁰

Nothing comparable is permitted as a legal matter or possible as a practical matter with respect to analogous but more traditional forms of communication. From a legal standpoint, under the Fourth Amendment the government may not, without a warrant, open and read letters sent through the mail in order to acquire those that contain particular information.⁵¹¹ Likewise, the government cannot listen to telephone conversations, without probable cause about one of the callers or about the telephone, in order to keep recordings of those conversations that contain particular content.⁵¹² And without the ability to engage in inspection of this sort, nothing akin to “about” collection could feasibly occur with respect to such traditional forms of communication. 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.

The government values “about” communications for the unique intelligence benefits that they can provide. Although we cannot discuss the details in an unclassified public report, the moniker “about” collection describes a number of distinct scenarios, which the government has in the past characterized as different “categories” of “about” collection. These categories are not predetermined limits that confine what the government acquires; rather, they are merely ways of describing the different forms of communications that are neither to nor from a tasked selector but nevertheless are collected because they contain the selector somewhere within them.⁵¹³ In some instances, the targeted person actually is a participant to the communication (using a different communications selector than the one that was “tasked” for collection), and so the term “about” collection may be misleading.⁵¹⁴ In other instances, a communication may not involve the targeted person, but for various logistical and technological reasons it will almost never involve a person located in the United States.

⁵¹⁰ See December 2011 Joint Statement, *supra*, at 7.

⁵¹¹ See *United States v. Jacobsen*, 466 U.S. 109, 114 (1984); *Ex parte Jackson*, 96 U.S. 727, 733 (1877).

⁵¹² See *Katz v. United States*, 389 U.S. 347 (1967).

⁵¹³ Such communications include “any Internet transaction that references a targeted selector, regardless of whether the transaction falls within one of the . . . previously identified categories of ‘about communications[.]’” Bates October 2011 Opinion, *supra*, at 31, 2011 WL 10945618, at *11.

⁵¹⁴ The term “*about*” communications was originally devised to describe communications that were “about” the selectors of targeted persons — meaning communications that contained such a selector within the communication. But the term has been used more loosely by officials in a way that suggests these communications are “about” the targeted persons. References to targeted *persons* do not themselves lead to “about” collection; only references to the communications *selectors* of targeted persons lead to “about” collection.

Some forms of “about” collection, however, do potentially intrude on the privacy of U.S. persons and people in the United States, as when, for instance, a U.S. person sends or receives an international communication to or from a non-target that contains a tasked email address in the body of the communication. Because selectors that are designated for collection under Section 702 need not be affiliated with any nefarious activity themselves, as explained earlier, a U.S. person’s use of a tasked selector in a communication does not necessarily indicate that the person is assisting a foreign power or engaged in any wrongdoing. Furthermore, that person’s communication will have been acquired because the government’s collection devices examined the *contents* of the communication, without the government having held any prior suspicion regarding that communication.

As noted above, however, all upstream collection — of which “about” collection is a subset — is “selector-based, i.e., based on . . . things like phone numbers or emails.”⁵¹⁵ Just as in PRISM collection, a selector used as a basis for upstream collection “is not a ‘keyword’ or particular term (e.g., ‘nuclear’ or ‘bomb’) but must be a specific communications identifier (e.g., email address).”⁵¹⁶ In other words, the government’s collection devices are not searching for references to particular topics or ideas, but only for references to specific communications selectors used by people who have been targeted under Section 702.

Moreover, the NSA’s acquisition of “about” communications is, to a large degree, an inevitable byproduct of its efforts to comprehensively acquire communications that are to or from its targets. Because of the specific manner in which the NSA conducts upstream collection, and the limits of its current technology, the NSA cannot completely eliminate “about” communications from its collection without also eliminating a significant portion of the “to/from” communications it seeks. Only to a limited degree could the agency feasibly turn off its “about” collection without incurring this result, and the outcome would not only represent an incomplete solution but would also undermine confidence that communications to and from targets are being reliably acquired. Additionally, there is no way at present for the NSA to selectively choose among the different categories of “about” communications at the collection stage. Nor does the NSA currently have any means available to automatically segregate “about” communications from “to/from” communications after collection, or to segregate among different forms of “about” communications after collection. Thus, ending all “about” collection would require ending even those forms of “about” collection that the Board regards as appropriate and valuable, and that have very little chance of impacting the privacy of people in the United States.

⁵¹⁵ PCLOB March 2014 Hearing Transcript, *supra*, at 26 (statement of Rajesh De, General Counsel, NSA); *see id.* (“This is not collection based on key words, for example.”); *id.* at 57 (“Abouts is a type of collection of information. . . . [A]ll collection of information is . . . focused on selectors, not key words . . . like terrorist, or like a generic name or things along those lines. . . . 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.”).

⁵¹⁶ NSA DCLPO REPORT, *supra*, at 4.

For now, therefore, “about” collection is an inextricable part of the NSA’s upstream collection, which we agree has unique value overall that militates against eliminating it entirely. As a result, any policy debate about whether “about” collection should be eliminated in whole or in part may be, to some degree, a fruitless exercise under present conditions. From our perspective, given a choice between the status quo and crippling upstream collection as a whole, we believe the status quo is reasonable. As explained later, however, because of the serious and novel questions raised by “about” collection as a constitutional and policy matter, we recommend that the NSA develop technology that would allow it to selectively limit or segregate certain forms of “about” communications — so that a debate can be had in which the national security benefits of the different forms of “about” collection are weighed against their respective privacy implications.

We emphasize, however, that our acceptance of “about” collection rests on the considerations described above — the inextricability of the practice from a broader form of collection that has unique value, and the limited nature of what “about” collection presently consists of: the acquisition of Internet communications that include the communications identifier of a targeted person. Although those identifiers may sometimes be found in the body of a communication, the government is not making any effort to obtain communications based on the ideas expressed therein. We are not condoning expanding “about” collection to encompass names or key words, nor to its use in PRISM collection, where it is not similarly inevitable. Finally, our unwillingness to call for the end of “about” collection is also influenced by the constraints that presently govern the use of such communications after acquisition. As with all upstream collection, “about” communications have a default retention period of two years instead of five, are not routed to the CIA or FBI, and may not be queried using U.S. person identifiers.

4. Multi-Communication Transactions (“MCTs”)

The technical means used to conduct the NSA’s upstream collection result in another issue with privacy implications. Because of the manner in which the agency intercepts communications directly from the Internet “backbone,” the NSA sometimes acquires communications that are not themselves authorized for collection (because they are not to, from, or “about” a tasked selector) in the process of acquiring a communication that *is* authorized for collection (because it is to, from, or “about” a tasked selector). In 2011, the FISA court held that the NSA’s procedures for addressing this problem were inadequate, and that without adequate procedures this aspect of the NSA’s collection practices violated the Fourth Amendment. The government subsequently altered its procedures to the satisfaction of the FISA court. Based on the Board’s assessment of how those procedures are being implemented today, the Board agrees that existing practices strike a reasonable balance between national security and privacy.

Unlike in PRISM collection, where the government receives communications from the Internet service providers who facilitate them, in upstream collection the NSA obtains what it calls “transactions” that are sent across the backbone of the Internet. Communications travel across the Internet in the form of data packets: a single email, for instance, can be broken up into a number of data packets that take different routes to their common destination, where they are reassembled to reconstruct the email. A complement of data packets, in NSA parlance, is a “transaction.”⁵¹⁷ These transactions will sometimes contain only a single, discrete communication, like a single email. At times, however, these transactions will contain a number of different individual communications. The NSA refers to the latter as an MCT.

An MCT is acquired by the NSA only if at least one individual communication within it meets the criteria for collection. That is, at least one of these individual communications must be to or from a tasked selector or contain reference to a tasked selector. But the MCT might also contain other individual communications that do not meet these criteria and that have no direct relationship to the tasked selector.⁵¹⁸ The NSA’s collection devices are unable to distinguish, before the point of acquisition, whether or not a transaction is an MCT. Thus, in the process of intercepting a communication that is “to/from” or “about” a tasked selector, the NSA might simultaneously obtain communications that are neither, because they are embedded within an MCT that contains a different communication meeting the standards for collection.⁵¹⁹ These other communications might be to or from U.S. persons or people located in the United States. They also might be domestic communications, *exclusively* between people located in the United States.

When the FISA court first began approving the Section 702 program in 2008, it did not understand that the NSA’s upstream process acquired “transactions” or that the agency was acquiring MCTs that included communications, including wholly domestic communications, that were not themselves authorized for collection. Only in 2011, after the government submitted a clarifying letter to the FISA court, did these aspects of upstream collection become clear to the court.⁵²⁰ After extensive briefing, a hearing, and the

⁵¹⁷ “The government describes an Internet ‘transaction’ as ‘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.’” Bates October 2011 Opinion, *supra*, at 28 n.23, 2011 WL 10945618, at *9 n.23.

⁵¹⁸ See December 2011 Joint Statement, *supra*, at 7.

⁵¹⁹ “About” collection and “MCT” collection are separate but overlapping categories. An MCT can be acquired if one of the communications within it is “about” a tasked selector (i.e., contains reference to a tasked selector), but an MCT also can be acquired if one of the communications within it is to or from a tasked selector. Thus, while “about” collection and “MCT” collection are both unique results of the upstream collection process, there is no inherent relationship between the two.

⁵²⁰ Bates October 2011 Opinion, *supra*, at 27-28, 30, 2011 WL 10945618, at *2, *9-11.

implementation of a study to estimate how many purely domestic communications were being acquired, the FISA court concluded that the NSA's practices were inconsistent with the Fourth Amendment and with the statutory requirement to minimize the retention of information about U.S. persons consistent with foreign intelligence needs. The FISA court accepted that the continued acquisition of MCTs was legitimate, but that the procedures in place to handle them after collection did not adequately protect the privacy interests of U.S. persons whose communications were acquired solely because they were contained within an MCT that also included a communication involving a tasked selector.

The government later resolved this issue to the FISA court's satisfaction by implementing new procedures for handling MCTs. Most notably, the NSA implemented procedures to segregate and restrict access to certain MCTs after collection, and established that any MCT found to contain a wholly domestic communication must be destroyed upon recognition. It also shortened the default retention period for communications acquired through upstream collection to two years.⁵²¹ These rules are now embodied in the NSA's minimization procedures. To address concerns about collection that occurred before these new procedures were implemented, the NSA later decided to purge all data in its repositories that it could identify as having been acquired through upstream before the date of these new procedures.⁵²²

The Board has inquired into how the NSA's new procedures for handling MCTs are being implemented, and it has learned — at a level of operational detail greater than what is reflected in the agency's minimization procedures — about the precise manner in which the segregation of MCTs occurs and the steps through which any use of a communication found in an MCT is permitted to occur. Based on this information, the Board believes that current practices adequately guard against the government's use of wholly domestic communications as well as other communications of U.S. persons that are not to, from, or about a tasked selector. Given the present impossibility of identifying, before collection, those MCTs that contain domestic communications or other U.S. persons' communications that are not themselves authorized for acquisition, we believe that the existing procedures strike a reasonable balance between national security and privacy. But we echo the FISA court's observation that it is incumbent upon the NSA to continue working to enhance its capability to limit its acquisitions to only targeted communications.⁵²³

⁵²¹ See Memorandum Opinion at 7-11, [*Caption Redacted*], [Docket No. Redacted], 2011 WL 10947772, at *3-5 (FISA Ct. Nov. 30, 2011), available at <http://icontherecord.tumblr.com/post/58944252298/dni-declassifies-intelligence-community-documents>.

⁵²² See Memorandum Opinion at 30, [*Caption Redacted*], [Docket No. Redacted], 2012 WL 9189263, at *3 (FISA Ct. Sept. 25, 2012), available at <http://www.dni.gov/files/documents/September%202012%20Bates%20Opinion%20and%20Order.pdf>.

⁵²³ See Bates October 2011 Opinion, *supra*, at 58 n.54, 2011 WL 10945618, at *20 n.54.

C. Retention, Use, and Dissemination of U.S. Persons' Communications under Section 702

Examining the privacy implications of the Section 702 program cannot end with a discussion of what is collected, but also must consider how information about U.S. persons is treated after collection: how long it is kept, who has access to it, in what ways it may be analyzed, under what circumstances it may be disseminated, and what procedures and oversight mechanisms are in place to ensure compliance with applicable rules.⁵²⁴

Once communications are acquired under Section 702, they go into one or more databases at the NSA, CIA, and FBI.⁵²⁵ At each agency, access to this Section 702 data is limited to those analysts or agents who have received training and guidance. In reviewing information contained in these databases, government personnel may come across communications involving U.S. persons. Data is frequently reviewed through queries, which identify communications that have particular characteristics specified in the query, such as containing a particular name or having been sent to or from a particular email address.⁵²⁶

Beginning first with inadvertent collection, if it is discovered that a Section 702 target is a U.S. person or was inside the United States at the time of targeting, the government must stop the collection immediately and generally must destroy any communications already acquired.⁵²⁷ While the imperative to stop collection is absolute, each agency is permitted, in limited circumstances, to waive the general requirement that communications already collected must be destroyed. At the NSA, for instance, the Director or Acting Director may waive the destruction requirement, on a communication-by-

⁵²⁴ Everything that is collected under Section 702 is treated as a “communication” and therefore is protected by the applicable minimization procedures.

⁵²⁵ The CIA and FBI each receive only a select portion of the communications acquired under Section 702, and they receive only Internet communications acquired through PRISM collection, not telephone calls or Internet communications acquired through upstream collection. The National Counterterrorism Center (“NCTC”) is not authorized to receive any unminimized Section 702 data, but instead has access to certain FBI systems containing minimized Section 702 data. The CIA holds all unminimized communications acquired through Section 702 in a standalone network that is separate from the CIA’s other information processing systems.

⁵²⁶ Because “about” and “MCT” collection occur only in upstream collection, which NSA alone receives, FBI and CIA personnel have no access to such communications.

⁵²⁷ See, e.g., 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, § 3(d)(2), 5 (Oct. 31, 2011) (“NSA 2011 Minimization Procedures”), available at <http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf>. If the government learns that a target who previously was outside the United States has traveled into the United States, it also must stop collection immediately, and it must generally destroy those communications that were acquired after the target entered the United States, subject to the possibility of a waiver discussed above. *Id.* § 3(d).

communication basis, by determining in writing that the communication satisfies one of several criteria. The destruction requirement may be waived if the communication is reasonably believed to contain “significant foreign intelligence information,” evidence of a crime, “technical data base information,” or “information necessary to understand or assess a communications security vulnerability.” Communications that indicate “a threat of serious harm to life or property” may also be preserved from destruction.⁵²⁸ The FBI standards are similar, as are the CIA standards, except that CIA waivers are limited to communications containing significant foreign intelligence or evidence of a crime.

Although approval for these waivers must come from the highest levels of the agencies, the breadth of the circumstances in which they can be approved raises concern that the waiver provisions might permit excessive use of communications that the agencies never should have acquired. Allowing the government to exploit the fruits of mistaken targeting decisions may risk creating an incentive for lax adherence to targeting restrictions. Presently, however, it appears that the government has been invoking these waiver provisions in a restrained manner. In 2013, for instance, the NSA Director waived the destruction of approximately forty communications (none of which was a wholly domestic communication), involving eight targets, based on a finding that each communication contained significant foreign intelligence information. Neither the CIA nor FBI utilized their waiver provisions in 2013. Along with the rigor that we believe is applied to the government’s determinations of foreignness during targeting, this sparing use of waivers helps to allay concern about their abuse. Furthermore, when an erroneous targeting was the result of a compliance incident, such as mistyping an email address, as opposed to a reasonable but mistaken belief about a target’s status, the waiver provision is unavailable.

Apart from communications acquired inadvertently, U.S. persons’ communications are not typically purged or eliminated from the government’s Section 702 databases before the end of their default retention periods, even when the communications pertain to matters unrelated to foreign intelligence or crime. This is because the agencies do not scrutinize each communication that they acquire or attempt to identify those that are to or from a U.S. person or person in the United States. The NSA’s minimization procedures, for instance, require the destruction of irrelevant communications of or concerning U.S. persons, but analysts are required to make such determinations only “at the earliest practicable point in the processing cycle,” and only where the communication can be identified as “clearly” not relevant to the purpose under which it was acquired or containing evidence of a crime.⁵²⁹ In practice, however, this destruction rarely happens. NSA analysts do not review all or even most communications acquired under Section 702

⁵²⁸ NSA 2011 Minimization Procedures, *supra*, § 5.

⁵²⁹ NSA 2011 Minimization Procedures, *supra*, § 3(b)(1).

as they arrive at the agency. Instead, those communications often remain in the agency's databases unreviewed until they are retrieved in response to a database query, or until they are deleted upon expiration of their retention period, without ever having been reviewed. Even when an analyst focuses on a particular communication, the destruction requirement is triggered only when analysts can affirm a negative: that the communication in question does *not* contain foreign intelligence or evidence of a crime.⁵³⁰ But communications that appear innocuous at first may later take on deeper significance as more contextual information is learned, and it can be difficult for one analyst to be certain that a communication has no intelligence value to any other analyst. As a matter of course, therefore, there is no routine deletion from the NSA's Section 702 databases of information that involves U.S. persons but is not pertinent to the agency's foreign intelligence mission. Therefore, although a communication must be "destroyed upon recognition" when an NSA analyst recognizes that it involves a U.S. person and determines that it clearly is not relevant to foreign intelligence or evidence of a crime,⁵³¹ in reality this rarely happens. Nor does such purging occur at the FBI or CIA: although their minimization procedures contain age-off requirements, those procedures do not require the purging of communications upon recognition that they involve U.S. persons but contain no foreign intelligence information.

Information that remains in the government's Section 702 databases may be queried to find the communications of specific U.S. persons under certain circumstances.⁵³² Queries are a key mechanism through which analysts access Section 702 information in the government's databases.⁵³³ They may involve "telephone numbers, key words or phrases, or other discriminators" as selection terms.⁵³⁴ Queries can be used to search both the content of communications and the addressing information, or "metadata," associated with the communications. At the NSA, content queries based on identifiers associated with specific U.S. persons — such as a name or email address — can be performed if they are "reasonably likely to return foreign intelligence information."⁵³⁵ No showing or suspicion is required that the U.S. person is engaged in any form of wrongdoing. In recent months, NSA analysts have performed queries using U.S. person identifiers to find information

⁵³⁰ NSA 2011 Minimization Procedures, *supra*, § 3(c). In addition, the communication must be "known" to contain information of or concerning U.S. persons. *Id.*

⁵³¹ NSA 2011 Minimization Procedures, *supra*, § 3(b)(1), (c)(1).

⁵³² The NSA and CIA first obtained approval to conduct queries using U.S. person identifiers in 2011. *See* Bates October 2011 Opinion, *supra*.

⁵³³ *See, e.g.*, NSA DCLPO REPORT, *supra*, at 6 ("[Analysts] access the information via 'queries,' which may be date-bound, and include alphanumeric strings such as telephone numbers, email addresses, or terms that can be used individually or in combination with one another.").

⁵³⁴ *See, e.g.*, NSA 2011 Minimization Procedures, *supra*, § 3(b)(6).

⁵³⁵ NSA 2011 Minimization Procedures, *supra*, § 3(b)(6); *see* NSA DCLPO REPORT, *supra*, at 7.

concerning, among other things, “individuals believed to be involved in international terrorism.” The CIA and FBI standards for content queries are essentially the same, except that the FBI, given its law enforcement role, is permitted to conduct queries to seek evidence of a crime as well as foreign intelligence information.

At the NSA, prior approval must be obtained to use content query terms that involve U.S. person identifiers. The agency records each term that is approved, though not the number of times any particular term is actually used to query a database. The NSA performs checks of its analysts’ queries. Prior approval is not required at the CIA; instead, the agency has developed audit capability. This system requires CIA personnel using U.S. person identifiers as query terms (or any other query term intended to return information about a particular U.S. person) write a contemporaneous foreign intelligence justification, which is documented along with a record of the query. Review of queries is also provided by the DOJ/ODNI oversight team, which reviews every U.S. person term approved for querying at the NSA as well as every U.S. person query performed at the CIA, reporting their numbers and any compliance issues to congressional oversight committees.

In 2013, the NSA approved the use of 198 terms involving U.S. person identifiers to perform content queries of its Section 702–acquired communications. During the same year, the CIA conducted approximately 1,900 queries of its unminimized Section 702–acquired communications, of which approximately forty percent were at the request of other U.S. intelligence agencies.⁵³⁶ Outside of those queries conducted on behalf of other intelligence agencies, CIA queries might involve, for instance, U.S. persons located overseas that intelligence indicates may be engaged in planning terrorist attacks or otherwise facilitating international terrorism.

While the FBI maintains records of content queries used to search its Section 702 data, it does not separately designate those that employ U.S. person identifiers, and so the number of U.S. person queries performed by the FBI is not known.

At the NSA, metadata queries, like content queries, must be reasonably designed to return foreign intelligence information when they involve U.S. person identifiers. Prior approval is not required, but the analyst must supply a written justification for the query, and all queries are recorded and subject to audit.⁵³⁷ The DOJ/ODNI oversight team reviews every NSA metadata query that involves a U.S. person identifier. In 2013, NSA analysts

⁵³⁶ Approximately 27 percent of these queries were duplicative of previous queries that employed the same query terms.

⁵³⁷ NSA DCLPO REPORT, *supra*, at 7.

performed approximately 9,500 queries of metadata acquired under Section 702 using U.S. person identifiers.⁵³⁸

The CIA also has the capability to conduct metadata-only queries against metadata derived from Section 702 collection. However, the CIA does not track how many metadata-only queries using U.S. person identifiers have been conducted. The CIA's minimization procedures do not contain any specific standard with respect to metadata queries involving U.S. person identifiers, although such queries are regulated under internal CIA regulations that govern queries of FISA and non-FISA information, and FISA itself requires that information collected be used only be for lawful purposes.⁵³⁹ The FBI requires that metadata queries, like content queries, be reasonably designed to return foreign intelligence or evidence of a crime. As noted above, however, the FBI does not separately track which of its queries involve U.S. person identifiers, and so the number of such metadata queries is not known.

As illustrated above, rules and oversight mechanisms are in place to prevent U.S. person queries from being abused for reasons other than searching for foreign intelligence or, in the FBI's case, for evidence of a crime. In pursuit of the agencies' legitimate missions, however, government analysts may use queries to digitally compile the entire body of communications that have been incidentally collected under Section 702 that involve a particular U.S. person's email address, telephone number, or other identifier, with the exception that Internet communications acquired through upstream collection may not be queried using U.S. person identifiers.⁵⁴⁰ In addition, the manner in which the FBI is employing U.S. person queries, while subject to genuine efforts at executive branch oversight, is difficult to evaluate, as is the CIA's use of metadata queries.

If the NSA, CIA, or FBI wishes to permanently retain a communication of or concerning a U.S. person (beyond the default retention periods), personnel must make a determination that retention is justified under certain criteria established in their minimization procedures. Those criteria demand a legitimate governmental interest in the communication, but are fairly broad with respect to the types of needs and purposes that justify retention. The NSA, for instance, permits retention if the identity of the U.S. person "is necessary to understand foreign intelligence information or asses its importance," or if

⁵³⁸ According to the DOJ/ODNI oversight team, the NSA's counting of its own metadata queries typically is overinclusive, often counting queries that do not actually include a U.S. person identifier as well as other queries where it is unclear whether a U.S. person identifier is involved.

⁵³⁹ See 50 U.S.C. §§ 1806(a).

⁵⁴⁰ See NSA 2011 Minimization Procedures, *supra*, § 3(b)(6).

the communication contains evidence of a crime, among other reasons.⁵⁴¹ The CIA's and FBI's rules are comparable.

Agencies that receive Section 702 communications may disseminate to another agency foreign intelligence information of or concerning a U.S. person, or evidence of a crime concerning a U.S. person, that was acquired from those communications. This is done most frequently by the NSA, reflecting the nature of its mission. When making such disseminations, NSA personnel typically “mask” the information about that U.S. person that could be used to identify him or her — replacing a proper name with, for instance, “a U.S. person” — but they may “unmask” such information upon request (with supervisory approval) when the requesting agency is deemed to legitimately require the information for its mission.⁵⁴² The number of disseminated reports containing references to U.S. person identifiers are reported annually to congressional oversight committees. As with U.S. person queries, these rules guard against the unjustified use of information about U.S. persons for illegitimate ends, but they do not significantly restrict the use of such information for legitimate intelligence and law enforcement aims.⁵⁴³

In 2013, the vast majority of the intelligence reports disseminated by the NSA that were based on intelligence derived from Section 702 contained no reference to any U.S. person. A significant number of such reports, however (albeit a small percentage of the total), did include references to U.S. persons. As noted, U.S. person information in these reports typically is initially “masked” to hide personally identifying information.

In response to requests from recipients of those reports (primarily intelligence and law enforcement agencies), last year the NSA “unmasked” approximately 10,000 U.S. person identities where the information was not included in the original reporting.⁵⁴⁴

Apart from this intelligence reporting, the NSA is permitted to pass on information showing possible violations of the law to the DOJ and the FBI. In 2013, the agency passed on such information only ten times.

⁵⁴¹ NSA 2011 Minimization Procedures, *supra*, § 6(a), (b)(2).

⁵⁴² NSA DCLPO REPORT, *supra*, at 7-8; NSA 2011 Minimization Procedures, *supra*, § 6(b).]

⁵⁴³ Under similar rules and additional internal restrictions, the NSA may share communications involving U.S. persons with foreign governments. NSA 2011 Minimization Procedures, *supra*, § 8(a). The NSA also is permitted to use and disseminate U.S. persons' privileged attorney-client communications, subject to approval from its Office of General Counsel, as long as the person is not known to be under criminal indictment in the United States and communicating with an attorney about that matter. *Id.* § 4. The CIA and FBI minimization procedures contain comparable provisions.

⁵⁴⁴ According to the NSA, fewer than a quarter of these identifiers were proper names of individuals or their titles; the remainder were U.S. corporation names, U.S. educational institution names, U.S.-registered IP addresses, websites hosted in the United States, email addresses or telephone numbers potentially used by U.S. persons, and other identifiers potentially used by U.S. persons.

In the Board's view, the protections contained in the agencies' minimization procedures are reasonably designed and implemented to ward against exploitation of information acquired under Section 702 for illegitimate purposes. The Board has seen no trace of any such illegitimate activity associated with the program, or any attempt to intentionally circumvent legal limits.

Depending on the scope of collection, however, the applicable rules may allow a substantial amount of private information about U.S. persons to be acquired by the government, examined by its personnel, and used in ways that may have a negative impact on those persons. Although it is not known how many communications involving U.S. persons or people in the United States are acquired under Section 702, the limited figures available may provide some indication of the extent to which the government presently could be using such communications. Some of these figures illustrate that the Section 702 program remains primarily focused on monitoring non-U.S. persons located outside the United States. By the same token, the overall scope of collection under the program and the quantity of intelligence reporting derived from this collection involving U.S. persons suggest that the government may be gathering and utilizing a significant amount of information about U.S. persons under Section 702.

If so, this would raise legitimate concern about whether a collection program that is premised on targeting foreigners located outside the United States without individual judicial orders now acquires substantial information about U.S. persons without the safeguards of individualized court review. Emphasizing again that we have seen no indication of abuse, nor any sign that the government has taken lightly its obligations to establish and adhere to a detailed set of rules governing the program, the collection and examination of U.S. persons' communications represents a privacy intrusion even in the absence of misuse for improper ends. The Board's desire to provide more clarity and transparency regarding the government's activities under Section 702, particularly insofar as they involve the acquisition and handling of U.S. persons' communications, underlies a number of our recommendations.

Part 6:

RECOMMENDATIONS

The Board has conducted an in-depth study of the Section 702 program. We have carefully considered whether the program as implemented complies with the statute and is consistent with constitutional requirements. The Board has also evaluated whether the program strikes the right balance between national security and privacy and civil liberties as a policy matter. The Board recognizes the considerable value that the Section 702 program provides in the government's efforts to combat terrorism and gather foreign intelligence, and finds that at its core, the program is sound. However, some features outside of the program's core, particularly those impacting U.S. persons, raise questions regarding the reasonableness of the program. The Board therefore offers a series of policy recommendations to ensure that the program includes adequate and appropriate safeguards for privacy and civil liberties.

The Board has identified five key areas where operations of the Section 702 program could strike a better balance between privacy, civil rights, and national security. They include the manner in which targeting and tasking is implemented, the manner in which queries using U.S. person identifiers are conducted, and the Foreign Intelligence Surveillance Court's ("FISC" or "FISA court") role in the certification process. Additional areas for improvement include the government's collection of upstream Internet transactions, transparency in the operations of the Section 702 program. We also make a recommendation, not limited only to Section 702, about evaluation of the efficacy of government surveillance programs. Based on our independent review and the conclusions we have drawn, the Board offers the following recommendations.

I. Targeting and Tasking

Recommendation 1: *The NSA's targeting procedures should be revised to (a) specify criteria for determining the expected foreign intelligence value of a particular target, and (b) require a written explanation of the basis for that determination sufficient to demonstrate that the targeting of each selector is likely to return foreign intelligence information relevant to the subject of one of the certifications approved by the FISA court. The NSA should implement these revised targeting procedures through revised guidance and training for analysts, specifying the criteria for the foreign intelligence determination and the kind of written explanation needed to support it. We expect that the FISA*

court's review of these targeting procedures in the course of the court's periodic review of Section 702 certifications will include an assessment of whether the revised procedures provide adequate guidance to ensure that targeting decisions are reasonably designed to acquire foreign intelligence information relevant to the subject of one of the certifications approved by the FISA court. Upon revision of the NSA's targeting procedures, internal agency reviews, as well as compliance audits performed by the ODNI and DOJ, should include an assessment of compliance with the foreign intelligence purpose requirement comparable to the review currently conducted of compliance with the requirement that targets are reasonably believed to be non-U.S. persons located outside the United States.

In order to target a person under Section 702, two basic criteria must be satisfied: the person must be a non-U.S. person located outside the United States (the “foreignness determination”) and the surveillance must be conducted to collect foreign intelligence information (the “foreign intelligence purpose determination”).

The Board's review of the Section 702 program showed that the procedures for documenting targeting decisions within the NSA, and the procedures for reviewing those decisions within the executive branch, focus primarily on the foreignness determination — establishing that a potential target is a non-U.S. person reasonably believed to be located abroad. The process for documenting and reviewing the foreign intelligence purpose of a targeting is not as rigorous. Agency personnel have not been required to articulate or explain these determinations in any detail as a matter of course, and typically indicate what category of foreign intelligence information they expect to obtain from targeting a particular person in a single brief sentence that contains only minimal information about why the analyst believes that targeting this person will yield foreign intelligence information. As a result, the Section 702 oversight team from the DOJ and the ODNI cannot scrutinize these foreign intelligence purpose determinations with the same rigor that it scrutinizes foreignness determinations. In contrast, NSA analysts are required to articulate a rationale to a much greater degree regarding their foreignness determinations, and oversight is accordingly more in-depth.

The Board recognizes that this distinction stems from the different treatment of the foreignness and foreign intelligence purpose determinations in Section 702 itself. Section 702(d), the subsection of the statute outlining the requirements for targeting procedures, specifically requires that the procedures be reasonably designed to ensure that targeting is limited to persons reasonably believed to be located outside the United States, but there is no comparable requirement in this subsection specifying that targeting procedures must be reasonably designed to ensure that targeting has a valid foreign intelligence purpose. Likewise, when the FISA court assesses whether the government's targeting procedures

comply with statutory requirements, the court is directed by Section 702(i), to consider the adequacy of those procedures with respect to the foreignness determination, but there is no comparable provision specifically requiring a review of the foreign intelligence purpose determination.

Despite the fact that the statute treats these two determinations differently, it also demands that *all* targeting be intended “to acquire foreign intelligence information.” Thus, the foreign intelligence purpose determination is a critical part of the statutory framework. From a constitutional perspective, moreover, at least insofar as Section 702 surveillance incidentally collects communications to and from U.S. persons, the foreign intelligence purpose is what provides the basis for the government to conduct Section 702 surveillance without a warrant. As a result, we conclude that there should be something closer to parity between the foreignness determination and foreign intelligence purpose determination in terms of what level of explanation is required of an analyst and how rigorous the oversight of that explanation is.

Therefore, the Board recommends that the NSA’s targeting procedures be updated to require a more detailed written explanation of the foreign intelligence purpose of each targeting decision and to specify the criteria that would be sufficient to demonstrate that this standard has been met. Changes to the targeting procedures that provide more guidance to analysts and require more explanation regarding the foreign intelligence purpose of a targeting will help analysts better articulate this element of their targeting decisions. When analysts articulate at greater length the bases for their targeting decisions, the executive branch oversight team that later reviews those decisions will be better equipped to meaningfully review them.

The Board does not believe that a statutory change is needed to implement this recommendation. The government already has the authority to amend its targeting procedures, subject to FISA court approval. We believe that it would be helpful for the FISA court, when reviewing Section 702 certifications, to assess whether the government’s targeting procedures are reasonably designed to ensure that targeting is limited to persons of foreign intelligence value, much like the court now assesses whether targeting procedures are reasonably designed to ensure that targeting is limited to persons located outside the United States. We believe that, without statutory change, the government could request that the FISA court assume this additional task, as the FISA court already must and does consider how fully the Section 702 program is geared toward acquiring foreign intelligence, in order to ensure that the program is authorized by the statute and consistent with the Fourth Amendment.

Once the revised targeting procedures are in place, analysts should be trained on their implementation, to ensure that the analysts are appropriately articulating the rationale for foreign intelligence purpose determinations. The NSA should also modify its

internal agency reviews to ensure that the new targeting procedures have been adopted by its analysts. The executive branch compliance audits should also be modified to reflect the new targeting procedures and to include more rigorous scrutiny of whether valid foreign intelligence purpose determinations are being properly articulated.

II. U.S. Person Queries

Recommendation 2: The FBI's minimization procedures should be updated to more clearly reflect actual practice for conducting U.S. person queries, including the frequency with which Section 702 data may be searched when making routine queries as part of FBI assessments and investigations. Further, some additional limits should be placed on the FBI's use and dissemination of Section 702 data in connection with non-foreign intelligence criminal matters.

When an FBI agent or analyst initiates a criminal assessment or begins a new criminal investigation related to any type of crime, it is routine practice, pursuant to the Attorney General Guidelines for Domestic FBI Operations, to conduct a query of FBI databases in order to determine whether they contain information on the subject of the assessment or investigation. The databases queried may include information collected under various FISA authorities, including data collected under Section 702. The FBI's rules relating to queries do not distinguish between U.S. persons and non-U.S. persons; as a domestic law enforcement agency, most of the FBI's work concerns U.S. persons. If a query leads to a "hit" in the FISA data (i.e., if a communication is found within a repository of Section 702 data that is responsive to the query), then the agent or analyst is alerted to the existence of the hit. If the agent or analyst has received training on how to handle FISA-acquired materials, he or she is able to view the Section 702 data that was responsive to the query; however, if the agent or analyst has not received FISA training he or she is merely alerted to the existence of the information but cannot access it. The agent or analyst would have to contact a FISA-trained agent or analyst and ask him or her to review the information.

Even though FBI analysts and agents who solely work on non-foreign intelligence crimes are not *required* to conduct queries of databases containing Section 702 data, they are *permitted* to conduct such queries and many do conduct such queries. This is not clearly expressed in the FBI's minimization procedures, and the minimization procedures should be modified to better reflect this actual practice. The Board believes that it is important for accountability and transparency that the minimization procedures provide a clear representation of operational practices. Among other benefits, this improved clarity will better enable the FISA court to assess statutory and constitutional compliance when

the minimization procedures are presented to the court for approval with the government's next recertification application.

In light of the privacy and civil liberties implications of using Section 702 information, collected under lower thresholds and for a foreign intelligence purpose, in the FBI's pursuit of non-foreign intelligence crimes, the Board believes it is appropriate to place some additional limits on what can be done with Section 702 information. Members of the Board differ on the nature of the limitations that should be placed on the use of that information. Board Members' proposals and a brief explanation of the reasoning supporting each are stated below, with elaboration in the two separate statements.

Additional Comment of Chairman David Medine and Board Member Patricia Wald

For acquisitions authorized under Section 702, FISA permits the FBI for law enforcement purposes, to retain and disseminate evidence of a crime. However, there is a difference between obtaining a U.S. person's communications when they are in plain view as an analyst reviews the target's communications, and the retrieval of a U.S. person's communications by querying the FBI's Section 702 holdings collected over the course of years.⁵⁴⁵ Therefore, consistent with our separate statement regarding Recommendation 3, we believe that U.S. persons' privacy interests regarding 702 data should be protected by requiring that each identifier should be submitted to the FISA court for approval before the identifier may be used to query data collected under Section 702, other than in exigent circumstances. The court should determine, based on documentation submitted by the government, whether the use of the U.S. person identifier for Section 702 queries meets the standard that the identifier is reasonably likely to return information relevant to an assessment or investigation of a crime. As discussed in more detail in our separate statement, this judicial review would not be necessary for U.S. persons who are already suspected terrorists and subject to surveillance under other government programs.

Additional Comment of Board Members Rachel Brand and Elisebeth Collins Cook

As explained in our separate statement, we would support a requirement that an analyst conducting a query in a non-foreign intelligence criminal matter obtain supervisory approval before accessing any Section 702 information that was responsive to the query. We would also support a requirement of higher-level Justice Department approval, to the extent not already required, before Section 702 information could be used

⁵⁴⁵ On June 25, 2014, the United States Supreme Court ruled unanimously that a search of a cell phone seized by the police from an individual who has been arrested required a warrant. *Riley v. California*, No. 13-132, 2014 WL 2864483 (U.S. June 25, 2014). The Court distinguished between reviewing one record versus conducting an extensive records search over a long period: "The fact that someone could have tucked a paper bank statement in a pocket does not justify a search of every bank statement from the last five years." *Id.* at *18. Likewise, observing evidence of a crime in one email does not justify conducting a search of an American's emails over the prior five years to or from everyone targeted under the Section 702 program.

in the investigation or prosecution of a non-foreign intelligence crime (such as in the application for a search warrant or wiretap, in the grand jury, or at trial). We would not require any additional approvals before an analyst could conduct a query of databases that include FISA data.

Additional Comment of Board Member James Dempsey

It is imperative not to re-erect the wall limiting discovery and use of information vital to the national security, and nothing in the Board's recommendations would do so. The constitutionality of the Section 702 program is based on the premise that there are limits on the retention, use and dissemination of the communications of U.S. persons collected under the program. The proper mix of limitations that would keep the program within constitutional bounds and acceptable to the American public may vary from agency to agency and under different circumstances. The discussion of queries and uses at the FBI in this Report is based on our understanding of current practices associated with the FBI's receipt and use of Section 702 data. The evolution of those practices may merit a different balancing. For now, the use or dissemination of Section 702 data by the FBI for non-national security matters is apparently largely, if not entirely, hypothetical. The possibility, however, should be addressed before the question arises in a moment of perceived urgency. Any number of possible structures would provide heightened protection of U.S. persons consistent with the imperative to discover and use critical national security information already in the hands of the government.⁵⁴⁶

Recommendation 3: The NSA and CIA minimization procedures should permit the agencies to query collected Section 702 data for foreign intelligence purposes using U.S. person identifiers only if the query is based upon a statement of facts showing that the query is reasonably likely to return foreign intelligence information as defined in FISA. The NSA and CIA should develop written guidance for agents and analysts as to what information and documentation is needed to meet this standard, including specific examples.

Under the NSA and CIA minimization procedures for the Section 702 program, analysts are permitted to perform queries of databases that hold communications acquired under Section 702 using query terms that involve U.S. person identifiers. Such queries are designed to identify communications in the database that involve or contain information relating to a U.S. person.

⁵⁴⁶ See Presidential Policy Directive — Signals Intelligence Activities, Policy Directive 28, 2014 WL 187435, § 2, (Jan. 17, 2014) (limiting the use of signals intelligence collected in bulk to certain enumerated purposes), available at <http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>.

The internal processes employed by the two agencies with respect to U.S. person queries differ. Under the NSA's minimization procedures, all queries that involve U.S. person identifiers (whether they search content or metadata) must be constructed so as to be "reasonably likely to return foreign intelligence information." The NSA also requires analysts to provide written justifications for the use of all query terms that involve U.S. person identifiers. More specifically, with respect to querying the metadata of Section 702 communications (which includes, for instance, the email address from which a communication was sent), analysts must document the basis for queries that involve U.S. person identifiers, which are subject to audit. With respect to queries that scan the contents of Section 702 communications, analysts must obtain prior approval for any query term that involves a U.S. person identifier. (Subsequent uses of an already approved query term do not require new permission.)

Under the CIA's minimization procedures, personnel must document the foreign intelligence basis for queries of content queries that involve U.S. person identifiers, which are subject to audit, but need not document a justification or obtain prior approval for queries of metadata.

Although the Board recognizes that NSA and CIA queries are subject to rigorous oversight by the DOJ's National Security Division and the ODNI (with the exception of metadata queries at the CIA, which are not reviewed by the oversight team), we believe that NSA and CIA analysts, before conducting a query involving a U.S. person identifier, should provide a statement of facts illustrating why they believe the query is reasonably likely to return foreign intelligence information.⁵⁴⁷ To assist in this process, the government should develop written guidance for the benefit of analysts who are authorized to perform such queries to clearly explain the meaning of the standard "reasonably likely to return foreign intelligence information." It should also provide illustrative examples of permissible and impermissible queries as well as proper and improper bases on which to conclude that a query is reasonably likely to return foreign intelligence. This guidance should reflect the fact that the statutory definition of "foreign intelligence information" under FISA is narrower when the information in question involves U.S. persons than it is when information pertains only to non-U.S. persons.

Implementing these measures will help to ensure that analysts at the NSA and CIA do not access or view communications acquired under Section 702 that involve or concern U.S. persons when there is no valid foreign intelligence reason to do so.

⁵⁴⁷ Board Member Elisebeth Collins Cook would not extend a new requirement to this effect to metadata queries.

III. FISC Role

Recommendation 4: To assist in the FISA court's consideration of the government's periodic Section 702 certification applications, the government should submit with those applications a random sample of tasking sheets and a random sample of the NSA's and CIA's U.S. person query terms, with supporting documentation. The sample size and methodology should be approved by the FISA court.

The FISA court reviews the government's proposed targeting and minimization procedures each time the government seeks approval or re-approval of a certification, typically annually. To assist the FISA court in its review, the government should provide the court with a random sample of targeting decisions (reflected in "tasking" sheets) and a random sample of NSA and CIA query terms that involve U.S. person identifiers.⁵⁴⁸ The FISC should approve the methodology used to select the samples and the size of those samples.

Providing a random sample of targeting decisions would allow the FISC to take a retrospective look at the targets selected over the course of a recent period of time. The data could help inform the FISA court's review process by providing some insight into whether the government is, in fact, satisfying the foreignness and foreign intelligence purpose requirements, and it could signal to the court that changes to the targeting procedures may be needed, or prompt inquiry into that question. The data could provide verification that the government's representations during the previous certification approval were accurate, and it could supply the FISC with more information to use in determining whether the government's acquisitions comply with the statute and the Fourth Amendment.

Similarly, a retrospective sample of U.S. person query terms and supporting documentation will allow the FISC to conduct a fuller review of the government's minimization procedures. Such a sample could allow greater insight into the methods by which information gathered under Section 702 is being utilized, and whether those methods are consistent with the minimization procedures. While U.S. person queries by the NSA and CIA are already subject to rigorous executive branch oversight (with the exception of metadata queries at CIA), supplying this additional information to the FISC could help guide the court by highlighting whether the minimization procedures are being followed and whether changes to those procedures are needed.

⁵⁴⁸ Chairman David Medine and Board Member Patricia Wald see no reason to exclude the FBI's query process from FISA court oversight. While it is correct that the FBI does not distinguish between queries using U.S. person identifiers and those that do not, as a domestic law enforcement agency it clearly conducts a significant number of queries using identifiers belonging to U.S. persons. Therefore, a sample of the queries performed by the FBI could inform the FISA court's review.

Recommendation 5: As part of the periodic certification process, the government should incorporate into its submission to the FISA court the rules for operation of the Section 702 program that have not already been included in certification orders by the FISA court, and that at present are contained in separate orders and opinions, affidavits, compliance and other letters, hearing transcripts, and mandatory reports filed by the government. To the extent that the FISA court agrees that these rules govern the operation of the Section 702 program, the FISA court should expressly incorporate them into its order approving Section 702 certifications.

The government's operation of the Section 702 program must adhere to the targeting and minimization procedures that are approved by the FISA court, as well as to the pertinent Attorney General guidelines and the statute itself. The government also makes additional representations to the FISA court through compliance notices and other filings, as well as during hearings, that together create a series of more rigorous precedents and a common understanding between the government and the court regarding the operation of the program. More than once, the government has implemented rules for the Section 702 program that are more detailed than what is reflected in the text of the targeting and minimization procedures themselves, although these rules typically are viewed as an interpretation of those procedures. These more detailed rules are not centrally located but are contained in compliance letters, affidavits, mandatory reports, hearing transcripts, and other sources that arise from the interaction between the government and the FISC. Such rules have precedential value and create real consequences, as the government considers itself bound to abide by the representations it makes to the FISA court. To the extent that the rules which have emerged from these representations and this interactive process govern the operation of the Section 702 program, they should be memorialized in a single place and incorporated into the FISC's certification review.

This recommendation is influenced by the Board's recognition that FISC judges and legal advisors do not serve on the court forever. As judges rotate out of FISC service, the risk that important information about the contours of the Section 702 program will be lost due to attrition, or not fully appreciated by new judges, greatly increases when the body of precedent that has developed over the course of the program's existence is not centrally located. Adopting this recommendation would ensure that each judge who may come to render decisions about the program will have ready access to a centralized source that encapsulates this body of precedent, to help inform his or her decisions and understanding of the program. This consolidation of rules will also facilitate congressional oversight of the Section 702 program. Accordingly, the Board views this recommendation as a measure to promote good government.

Additionally, incorporating the series of precedents described above into a comprehensive source will provide a single reference point for every government lawyer, agent, officer, and analyst within the Intelligence Community who has responsibilities under the Section 702 program. These precedents and rules, given their dispersed location within a range of different FISA court filings and documents, may not be readily accessible to the lawyers tasked with helping to implement the requirements specified in those documents or to the agents and analysts operating the program. A complete, readily accessible legal framework will assist lawyers and analysts throughout the government in their efforts to comply with the requirements of the Section 702 program.

IV. Upstream and “About” Collection

Recommendation 6: To build on current efforts to filter upstream communications to avoid collection of purely domestic communications, the NSA and DOJ, in consultation with affected telecommunications service providers, and as appropriate, with independent experts, should periodically assess whether filtering techniques applied in upstream collection utilize the best technology consistent with program needs to ensure government acquisition of only communications that are authorized for collection and prevent the inadvertent collection of domestic communications.

In PRISM collection, through which the government obtains communications directly from Internet service providers, the government acquires only those communications sent to or from selectors used by targeted persons. Obtaining only communications sent to and from those selectors helps ensure that no wholly domestic communications are acquired — because the targeted person who uses the selector always must be someone reasonably believed to be located outside the United States.

In upstream collection, by contrast, the NSA obtains communications directly from the Internet “backbone,” with the compelled assistance of companies that maintain those networks, rather than Internet service providers that supply particular modes of communication. The success of this process depends on collection devices that can reliably acquire data packets associated with the proper communications. In addition, through “about” collection, the upstream process includes acquiring communications that contain reference to selectors used by targeted persons, even if the communication is not sent to or from the account of that selector. Because the targeted person may not be a party to the communication, it is possible that neither participant in the communication is located outside the United States, although the NSA takes additional measures, including the use of IP filters, to try to avoid collecting wholly domestic communications.

As a result, upstream collection involves a greater risk that the government will acquire wholly domestic communications, which it is not authorized to intentionally collect under Section 702. Ensuring that the upstream collection process comports with statutory limits and with agency targeting procedures involves an important technical process of filtering out wholly domestic communications. The government acknowledges, however, that the technical methods used to prevent the acquisition of domestic communications do not completely prevent them from being acquired. Even if domestic communications were to constitute a very small percentage of upstream collection, this could still result in a large overall number of purely domestic communications being collected. Mindful of these considerations, the Board believes that there should be an ongoing dialogue, both within the government and in cooperation with telecommunications providers or independent experts, to ensure that the means being used to filter for domestic communications use the best technology. We also believe that the determination about whether this is the case should be continually revisited.

Recommendation 7: The NSA periodically should review the types of communications acquired through “about” collection under Section 702, and study the extent to which it would be technically feasible to limit, as appropriate, the types of “about” collection.

In the upstream collection process, as in the PRISM collection process, the NSA acquires Internet communications sent to and from the selector, such as an email address, used by a targeted person. In upstream, however, the NSA also acquires Internet communications that are not sent to or from this email address, but instead contain reference to the selector, sometimes in the body of the communication. These are termed “about” communications, because they are not to or from, but rather “about” the communication selectors of targeted persons. In addition, for technical reasons, “about” collection is needed even to acquire some communications that actually are “to” or “from” a target.

A number of different scenarios result in a communication containing reference to a particular selector when the communication is not to or from that selector. Thus, there are a number of different categories or types of “about” communications acquired by the NSA. Some forms of “about” communications are actually the communications of targeted persons. Other types of “about” collection can result in the acquisition of communications between two non-targets, thereby implicating greater privacy concerns. For instance, when a person in the United States sends or receives an international communication that contains a targeted email address in the body of the communication, that communication may be acquired by the NSA, even if the sender and recipient are not targets themselves and were completely unknown to the government before its collection devices examined

the contents of their communication. Moreover, the permissible scope of targeting in the Section 702 program is broad enough that targets need not themselves be suspected terrorists or other bad actors. Thus, if the email address of a target appears in the body of a communication between two non-targets, it does not necessarily mean that either of the communicants is in touch with a suspected terrorist.

All of these types of “about” communications can provide intelligence value, helping the government learn more about terrorist networks and their plans or obtain other foreign intelligence. While “about” collection is valued by the government for its unique intelligence benefits, it is, to a large degree, an inevitable byproduct of the way the NSA conducts much of its upstream collection. As discussed earlier in this Report, because of the technical manner in which this collection is performed, the NSA cannot entirely stop acquiring “about” communications without also missing a significant portion of “to/from” communications. Nor does the agency have the capability to selectively acquire certain types of “about” communications but not others.

At least some forms of “about” collection present novel and difficult issues regarding the balance between privacy and national security. But current technological limits make any debate about the proper balance somewhat academic, because it is largely unfeasible to limit “about” collection without also eliminating a substantial portion of upstream’s “to/from” collection, which would more drastically hinder the government’s counterterrorism efforts.

We therefore recommend that the NSA work to develop technology that would enable it to identify and distinguish among the types of “about” collection at the acquisition stage, and then selectively limit or modify its “about” collection, as may later be deemed appropriate. If it is not possible for collection devices to identify or differentiate among types of “about” communications at the acquisition stage, we urge the NSA to develop technology that would allow it to automatically segregate all “about” communications after collection (and, if possible, to individually segregate different types of “about” communications from one another after collection). With such mechanisms in place, it will be possible to have a policy discussion about whether or not the privacy impacts of particular types of “about” collection justify treating those types of communications in a different way or eliminating their collection entirely.

V. Accountability and Transparency

Recommendation 8: To the maximum extent consistent with national security, the government should create and release, with minimal redactions, declassified versions of the FBI’s and CIA’s Section 702 minimization procedures, as well as the NSA’s current minimization procedures.

The Board believes that the public would benefit from understanding the procedures that govern the acquisition, use, retention, and dissemination of information collected under Section 702. The Board respects the government's need to protect its operational methods and practices, but it also recognizes that transparency enables accountability to the public that the government serves. Therefore, the Board urges the government to engage in a declassification review and, to the greatest extent possible without jeopardizing national security, release unredacted versions of the FBI, CIA, and NSA minimization procedures.

Recommendation 9: The government should implement five measures to provide insight about the extent to which the NSA acquires and utilizes the communications involving U.S. persons and people located in the United States under the Section 702 program. Specifically, the NSA should implement processes to annually count the following: (1) the number of telephone communications acquired in which one caller is located in the United States; (2) the number of Internet communications acquired through upstream collection that originate or terminate in the United States; (3) the number of communications of or concerning U.S. persons that the NSA positively identifies as such in the routine course of its work; (4) the number of queries performed that employ U.S. person identifiers, specifically distinguishing the number of such queries that include names, titles, or other identifiers potentially associated with individuals; and (5) the number of instances in which the NSA disseminates non-public information about U.S. persons, specifically distinguishing disseminations that includes names, titles, or other identifiers potentially associated with individuals. These figures should be reported to Congress in the NSA Director's annual report and should be released publicly to the extent consistent with national security.

Under Section 702, the government acquires the contents of telephone calls and Internet communications from within the United States, without individualized warrants or court orders, so long as the acquisition involves targeting non-U.S. persons reasonably believed to be located outside the United States, for foreign intelligence purposes.

Those targeted persons, of course, may communicate with U.S. persons or people located in the United States, resulting in the "incidental" collection of their communications. Since the enactment of the FISA Amendment Act in 2008, the extent to which the government acquires the communications of U.S. persons under Section 702 has been one of the biggest open questions about the program, and a continuing source of public concern. Lawmakers and civil liberties advocates have called upon the executive branch to disclose how many communications of U.S. persons are being acquired. In turn,

the executive branch has responded that it cannot provide such a number — because it is often difficult to determine from a communication the nationality of its participants, and because the large volume of collection under Section 702 would make it impossible to conduct such determinations for every communication that is acquired. The executive branch also has pointed out that any attempt to document the nationality of participants to communications acquired under Section 702 would actually be invasive of privacy, because it would require government personnel to spend time scrutinizing the contents of private messages that they otherwise might never access or closely review.

As a result of this impasse, lawmakers and the public do not have even a rough estimate of how many communications of U.S. persons are acquired under Section 702.

Based on information provided by the NSA, the Board believes that certain measures can be adopted that could provide insight into these questions without unduly burdening the NSA or disrupting the work of its analysts, and without requiring the agency to further scrutinize the contents of U.S. persons' communications. We believe that the NSA could implement five measures, listed above, that collectively would shed some light on the extent to which communications involving U.S. persons or people located in the United States are being acquired and utilized under Section 702. While the measures we have proposed will provide only partial insight into this question (they will not, for instance, reveal the number of communication obtained under PRISM collection, which accounts for the vast majority of Internet acquisitions), they will provide a snapshot, albeit imperfect, of the degree to which the NSA under Section 702 acquires communications involving U.S. persons, queries them, retains them permanently, and disseminates information from them to other agencies.

The number of queries and disseminations involving U.S. person information are already tracked by the NSA, but we believe that these figures should be annually reported in a central document along with the new figures we have proposed counting, and that the NSA's annual reporting of its queries and disseminations should highlight those that potentially involve *individuals* (as opposed to businesses or institutions), which are of special interest from a privacy perspective. It is possible that with respect to the first two measures above, the information that the NSA feasibly can document might turn out to be insufficiently comprehensive to yield dependable numbers, but this will not be known until the NSA attempts to implement the recommendation.

Adopting the measures that we have proposed will supply policymakers and the public with important information about one of the most frequently discussed aspects of the Section 702 program, enabling more informed judgments to be made about the program in the future.

VI. Efficacy

Recommendation 10: The government should develop a comprehensive methodology for assessing the efficacy and relative value of counterterrorism programs.

The efficacy of any particular counterterrorism program is difficult to assess. Even when focusing only on programs of *surveillance*, such programs can serve a variety of functions that contribute to the prevention of terrorism. Most obviously, a surveillance program may reveal the existence of a planned terrorist attack, enabling the government to disrupt the attack. But the number of “plots thwarted” in this way is only one measure of success. Counterterrorism surveillance programs can enable the government to learn about the identities and activities of the individuals who make up terrorist networks. They can help the government to understand the goals and intentions of those organizations, as well as the ways in which the organizations fund their pursuits and coordinate the activities of their members. All of this knowledge can aid the government in taking steps to frustrate the efforts of these terrorist organizations — potentially stymieing their endeavors long before they coalesce around the plotting and implementation of a specific attack. Because the nature of counterterrorism efforts can vary, measures of success may vary as well.

Moreover, individual counterterrorism programs are not typically used in isolation; rather, these programs can support and mutually reinforce one another. Therefore, the success of a particular program may not be susceptible to evaluation based on what it produces in a vacuum. Any evaluation must instead seek to understand how a particular program fits within the government’s overall counterterrorism efforts, and to what degree it aids those efforts relative to other programs.

Despite these complications, determining the efficacy and value of particular counterterrorism programs is critical. Without such determinations, policymakers and courts cannot effectively weigh the interests of the government in conducting a program against the intrusions on privacy and civil liberties that it may cause. In addition, government counterterrorism resources are not unlimited, and if a program is not working, those resources should be redirected to programs that are more effective in protecting us from terrorists. Accordingly, the Board believes that the government should develop a methodology to gauge and assign value to its counterterrorism programs, and use that methodology to determine if particular programs are meeting their stated goals. The Board is aware that the ODNI conducts studies to measure the relative efficacy of different types of intelligence activities to assist in budgetary decisions. The Board believes that this important work should be continued, as well as expanded so as to differentiate more precisely among individual programs, in order to assist policymakers in making informed, data-driven decisions about governmental activities that have the potential to invade the privacy and civil liberties of the public.

Part 7:

CONCLUSION

One of the Board's goals in developing this Report has been to provide greater transparency and clarity to the public regarding the operation of the Section 702 program. This is a complex program, and, in the wake of the unauthorized disclosures about the program, there has been a great deal of misinformation circulated to the public. The Board is grateful to the Intelligence Community and the Department of Justice for its employees' tireless efforts to educate Board Members and staff about the program's operation, and to work with us to declassify information in the public interest. The Board also appreciates the work of the many government officials and employees, congressional staff, privacy and civil liberties advocates, academics, trade associations, and technology and communications companies who provided input into the Board's study of the program.

In addition to this effort to explain the Section 702 program, the Board has set forth a series of policy recommendations designed to ensure that the program appropriately balances national security concerns with privacy and civil liberties. We note that this is only the start of the dialogue. We do not believe that any of the recommendations we offer would require legislative changes, and the Board welcomes the opportunity for further discussion of these pressing issues and how to best implement the Board's recommendations. We hope that this Report contributes to "a way forward that secures the life of our nation while preserving the liberties that make our nation worth fighting for."⁵⁴⁹

⁵⁴⁹ Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014), *available at* <http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence>.

INDEX TO ANNEXES

- A. Separate Statement by Chairman David Medine and Board Member Patricia Wald
- B. Separate Statement by Board Members Rachel Brand and Elisebeth Collins Cook
- C. July 9, 2013 Workshop Agenda and Link to Workshop Transcript
- D. November 4, 2013 Hearing Agenda and Link to Hearing Transcript
- E. March 19, 2014 Hearing Agenda and Link to Hearing Transcript
- F. Request for Public Comments on Board Study
- G. Reopening the Public Comment Period
- H. Index to Public Comments on www.regulations.gov

ANNEX A

Separate Statement of Chairman David Medine and Board Member Patricia Wald

I. Recommendation Regarding U.S. Person Queries for Foreign Intelligence Purposes

We do not believe that the Board's Recommendation 3 goes nearly far enough to protect U.S. persons' privacy rights when their communications are incidentally collected as a consequence of targeting a non-U.S. person located abroad under Section 702. The Section 702 program has collected hundreds of millions of Internet communications. Even if only a small percentage of those communications are to or from an American, the total number of Americans' communications is likely significant. Furthermore, these communications, which may be maintained for many years in government databases in searchable form, may contain sensitive and confidential matters having nothing to do with the foreign intelligence purposes of the Section 702 program. Although such queries must be conducted for a foreign intelligence purpose, currently, the government can query several years of such communications without court approval, which could potentially produce a composite picture of a significant slice of an American's private life.

This practice raises two related concerns with constitutional, statutory, and policy implications. First, are sufficient protections in place to purge Americans' communications that have no foreign intelligence value? Second, are there sufficient restrictions on when the government can query data collected under Section 702 to seek Americans' communications? We offer the following proposals to address each of these concerns.

Recommendation

Minimization procedures that govern the use of Americans' communications collected under Section 702 should require the following:

(1) No later than when the results of a U.S. person query of Section 702 data are generated, Americans' communications should be purged of information that does not meet the statutory definition of foreign intelligence information relating to Americans.⁵⁵⁰ This process should be subject to judicial oversight.

(2) Each U.S. person identifier should be submitted to the FISA court for approval before the identifier may be used to query data collected under Section 702 for a foreign

⁵⁵⁰ U.S. person communications may also be responsive to queries using non-U.S. person identifiers. The same purge procedure should apply in such cases.

intelligence purpose,⁵⁵¹ other than in exigent circumstances or where otherwise required by law.⁵⁵² The court should determine, based on documentation submitted by the government, whether the use of the U.S. person identifier for Section 702 queries meets the standard that the identifier is reasonably likely to return foreign intelligence information as defined under FISA.⁵⁵³

Discussion

As explained in Part 3 above, under Section 702, the government may lawfully collect the communications of an American where that individual is communicating with a targeted non-U.S. person who is reasonably believed to be located outside the United States.⁵⁵⁴ The government refers to the collection of such Americans' information as "incidental" collection, because the American will not be, and cannot be, the target of Section 702 surveillance. Although we understand that the government does not currently count the number of incidentally collected American communications, it is likely that the scope and extent of the Americans' information collected under Section 702 is substantial: as of 2011, the NSA was acquiring approximately 250 million Internet communications annually, and even if only a small percentage of these total involved Americans the number would be large in absolute terms.⁵⁵⁵

We recognize that a query of collected Section 702 data seeking information about a specific American⁵⁵⁶ may not provide as complete a picture of the individual's activities as it would for an actual target of surveillance. Nonetheless, such queries are capable of

⁵⁵¹ Queries for criminal purposes are governed by the proposal in Part II of this statement.

⁵⁵² See, e.g., *Brady v. Maryland*, 373 U.S. 83 (1963); Fed. R. Crim. P. 16 (a)(1)(B); and 18 U.S.C. § 3500 (Jenks Act).

⁵⁵³ Subsequent queries using a FISA court-approved U.S. person identifier would not require court approval.

⁵⁵⁴ Through "about" collection, the NSA may also collect the communication of an American who is not in direct contact with a Section 702 target if a targeted selector appears within the communication. In addition, the NSA may collect the communications of an American who is not in direct contact with a Section 702 target through acquiring an "MCT." However, such communications are acquired only through upstream collection and, thus, they may not be queried using U.S. person identifiers under current minimization procedures.

⁵⁵⁵ The NSA minimization procedures state that permanent retention of communications of Americans is permitted if they are of foreign intelligence value or certain other standards are met, including communications in which the identity of the American is necessary to understand foreign intelligence information or assess its importance. 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, § 6(b)(2) (Oct. 31, 2011) ("NSA 2011 Minimization Procedures").

⁵⁵⁶ We are not proposing that the parties to every communication be investigated to determine if one or more of the parties are Americans. Such reviews themselves could raise privacy and civil liberties concerns. However, where there is a reasonable basis to conclude that a party is an American, the recommended procedures should apply.

revealing a significant slice of the American's life. This is particularly the case for Americans who correspond frequently with foreigners, including relatives, business associates, and others. Because the scope of the legitimate foreign intelligence purposes that may justify surveillance under Section 702 is broad, going beyond counterterrorism, an American could be in contact with several targets of Section 702 surveillance and yet be innocent of any complicity in terrorist or other activity of foreign intelligence interest. Since Section 702 does not require any particularized judicial finding to support the initial collection of information from either the foreign target or the American who communicated with the target, further safeguards should be required to limit the permissible scope of U.S. person queries. Under present rules, querying of the communications to which the American was a party can be justified either on the grounds that they are likely to have foreign intelligence value or contain evidence of a crime.⁵⁵⁷ Moreover, there is currently no external check outside of the executive branch on the process of making such queries or purging of non-foreign intelligence material from query results.

We agree that legitimate foreign intelligence matters which appear in these Americans' incidentally collected communications can be retained. However, we feel strongly that the present internal agency procedures for reviewing communications and purging those portions that are of no foreign intelligence value prior to use of the information⁵⁵⁸ are wholly inadequate to protect Americans' acknowledged constitutional rights to protection for private information or to give effect to the statutory definition of foreign intelligence information, which, as discussed below, provides a more stringent test for information relating to Americans. Minimization guidelines approved by the FISA court were intended to afford these protections, but in their present form they do not. As a practical matter, most collected communications are not reviewed for the purging of non-foreign intelligence matters upon collection, or at any set time thereafter prior to use. The NSA guidelines require only that "upon review" the analyst should purge material that is "clearly" non-foreign intelligence information. The practice, when applying the "clearly" criteria for purging Americans' communications, is to err on the side of insuring that any piece of private information is retained that might in the future conceivably take on value or that some other analyst in the intelligence community might find to be of value. We do not think this is the intent of the statute.

Some argue that the process of reviewing and purging of private information that has no intelligence value is more intrusive than permitting the information to remain in agency databases for years subject to viewing by intelligence personnel in multiple

⁵⁵⁷ See Section II of this Separate Statement regarding FBI queries relating to evidence of a crime.

⁵⁵⁸ NSA 2011 Minimization Procedures, *supra*, § 3.

agencies. In our view, there is no legitimate basis to maintain potentially personal, sensitive information that has no bearing on either foreign intelligence or criminal conduct. Nor do the restrictions on use of FISA data in criminal investigations requiring only Attorney General approval provide adequate protections to the vast majority of Americans whose communications have been incidentally collected, who will never be subjected to such proceedings, but whose information can be probed and queried and used to pursue investigations against them.

Our conclusion that more controls are required for this query process is informed by constitutional, statutory, and policy concerns. As discussed above, under the Fourth Amendment, the reasonableness of this program must be assessed based on the totality of the circumstances.⁵⁵⁹ The government recognizes that the initial collection of Americans' communications under Section 702 constitutes a search under the Fourth Amendment. The reasonableness of this surveillance depends upon whether there are sufficient safeguards, including targeting and minimization procedures, to adequately protect the Fourth Amendment interests of persons whose communications may be collected, used, and disseminated. Since there are no prior determinations that any Americans whose communications have been collected are involved in terrorism or other activities of foreign intelligence interest (because Americans cannot be targeted), there should be compensatory safeguards governing the access, use, dissemination, and retention of the contents of their communications when those communications are acquired in the course of targeting others.

In this regard, we do not believe that the Fourth Amendment analysis justifying, in other contexts, the use of queries directed at individuals who are not themselves surveillance targets applies with equal force to querying U.S. person communications acquired in the Section 702 program. As discussed above, the incidental collection of information through a Title III wiretap meets Fourth Amendment standards based on the prior judicial review, showing of probable cause, and particularity in the wiretap order, which justifies the surveillance both with respect to known suspects and with respect to incidental interceptees.⁵⁶⁰ Under Section 702, by contrast, there is no probable cause or other individualized finding by a judge — either with regard to the non-U.S. person who is the target of the surveillance or the American who communicates with the target. Nor is there any judicial review after the fact of targeting decisions or queries. It is troubling to allow the government without some form of judicial approval to compile and review private communications by U.S. persons who have not consented to the government's collection. To address these constitutional concerns, more robust safeguards should be

⁵⁵⁹ *Samson v. California*, 547 U.S. 843, 848 (2006).

⁵⁶⁰ *United States v. Donovan*, 429 U.S. 413, 427 n.15 (1977).

required at the query stage, whenever the government seeks to conduct queries seeking information about U.S. person's communications, in order to support the reasonableness of the program. Existing query standards, which require no outside review, are insufficient to compensate for the lack of judicial review at the front end so as to provide assurance about the legitimacy and scope of the collection. On the other hand, judicial review would not be necessary for queries seeking communications of U.S. persons who are already approved as targets for collection under Title I or Sections 703/704 of FISA and identifiers that have been approved by the FISA court under the "reasonable articulable suspicion" standard for telephony metadata under Section 215.⁵⁶¹ As a result, this would not restrict queries regarding U.S. persons who are already suspected terrorists and are under surveillance.

The statutory framework of FISA further supports the need for enhanced safeguards for U.S. person information. The definition of foreign intelligence information under FISA, which is incorporated by reference into Section 702, sets forth several categories of information, including information regarding international terrorism or international proliferation of weapons of mass destruction. To meet the statutory definition, the information generally must "*relate to*" one of the listed categories, but if the information concerns a U.S. person, the definition specifically requires that the information must "*be necessary to*" the ability of the United States to protect against these threats.⁵⁶² At the query stage, this definition is relevant because the NSA minimization procedures require that queries using U.S. person identifiers must be reasonably likely to return foreign intelligence information. We believe that foreign intelligence information in the query context must track the statutory definition, which, for U.S. persons, involves the higher "necessary" standard.

When FISA was originally enacted, Congress made clear in passing the statute that enhanced safeguards were needed for U.S. person information. As the report of the House Permanent Select Committee on Intelligence explained:

[T]he committee has adopted a definition of foreign intelligence information which includes any information relating to these broad security or foreign relations concerns, so long as the information does not concern U.S. persons. Where U.S. persons are involved, the definition is much stricter; it requires that the information be "necessary" to these security or foreign relations concerns.

⁵⁶¹ It would also not be necessary if the query produces no results or the analyst purges all results from the given query as not containing foreign intelligence.

⁵⁶² 50 U.S.C. § 1801(e) (emphasis added).

Where the term “necessary” is used, the committee intends to require more than a showing that the information would be useful or convenient. The committee intends to require a showing that the information is both important and required. The use of this standard is intended to mandate that a significant need be demonstrated by those seeking the surveillance. For example, it is often contended that a counterintelligence officer or intelligence analyst, if not the policymaker himself, must have every possible bit of information about a subject because it might provide an important piece of the larger picture. In that sense, any information relating to the specified purposes might be called “necessary” but such a reading is clearly not intended.⁵⁶³

To give effect to this definition of foreign intelligence information under FISA, and the cautionary words from both the House and Senate reports, we believe that the approval process for U.S. person queries under Section 702 must be tightened. The more stringent “necessity” test for foreign intelligence information relating to U.S. persons requires that queries seeking to identify incidentally collected communications of an American must be reasonably designed to produce information necessary to the ability of the United States to protect against the listed threats, or to assure the defense or security of the United States or the conduct of its foreign affairs. It is imperative that a process be instituted to assure compliance with this definition.

Finally, as a policy matter, we seek to find the appropriate balance that will enable the government to pursue its legitimate foreign intelligence purposes while still safeguarding legitimate privacy interests. The government urges that once information has been lawfully collected, it may be used for any lawful purposes, and that existing minimization rules under Section 702 provide sufficient safeguards against improper use. In contrast, on June 19, 2014, the U.S. House of Representatives, by a 293-to-123 bipartisan vote, approved a ban on U.S. person queries under Section 702.⁵⁶⁴ The President’s Review Group on Intelligence and Communications Technologies, many advocacy organizations, certain members of Congress, and others have urged that in order to conduct a U.S. person query of Section 702 data, the government should be required to obtain a FISA warrant under Title I of the statute and demonstrate probable cause that the U.S. person is a foreign power or an agent or employee of a foreign power. Last week, a federal district court judge noted that whether the Fourth Amendment requires a warrant for queries to be conducted

⁵⁶³ H.R. Rep. No. 95-1283, at 47 (1978); *see also* S. Rep. No. 95-701, at 31 (1978) (containing similar language).

⁵⁶⁴ The ban applies to agencies that would be funded under the proposed Defense Appropriations Act, 2015 (H.R. 4870), which would not include the FBI. *See* H.Amdt.935, 113th Cong. (2014), 160 CONG. REC. H5,544 (daily ed. June 19, 2014), *available at* <http://www.gpo.gov/fdsys/pkg/CREC-2014-06-19/pdf/CREC-2014-06-19.pdf>.

of Section 702 data was “a very close question.”⁵⁶⁵ He ultimately ruled the Fourth Amendment did not require a warrant even though such a requirement might “better protect Americans’ privacy rights.” We believe that the middle course we propose — not banning queries or requiring a warrant but instead requiring judicial approval of queries employing a more relaxed standard — more appropriately balances the government’s legitimate foreign intelligence purposes with the privacy rights of Americans.

With regard to query results, it is important on both legal and policy grounds for the government to implement procedures under which Section 702 communications are reviewed to assess whether they meet the statutory definition of foreign intelligence information applicable to U.S. persons no later than when the results of a U.S. person query are generated, to insure that only those meeting the “necessary” standard are used, retained or disseminated and those not meeting the definition are purged.⁵⁶⁶ At base we believe some external oversight of the review process is essential to counteract an understandable but strong reluctance of analysts to give up any information that might conceivably have some future remote value, despite the more restrictive statutory definitions of foreign intelligence for Americans’ information.⁵⁶⁷

While we conclude that a particularized judicial finding should be required *before* a U.S. person query has been made, to ensure that it has a proper basis, we believe the FISA Title I standard for targeting is too demanding in the query context. Rather, the

⁵⁶⁵ *United States v. Mohamud*, No. 10-475, 2014 WL 2866749 at *26 (D. Or. June 24, 2014).

⁵⁶⁶ We recognize that some communications of Americans may never be returned as the result of a query or otherwise reviewed before they are “aged-off” of agency systems at the end of the data retention period.

⁵⁶⁷ One alternative in that regard would be for the FISA court to use a special master with a security clearance to regularly review representative samples of query results. The master would assess whether information that does not meet the statutory definition of foreign intelligence information had been properly purged and report to the court on the master’s findings. *See In re U.S. Dep’t of Defense*, 848 F.2d 232, 239 (D.C. Cir. 1988) (“[W]here a massive number of classified documents exists such that the judge and his law clerk simply cannot examine them all . . . appointment of a master to structure the judge’s review of these documents is appropriate so long as the judge retains decisional authority over the issue in question.”). If the FISA court concluded over time that the review and purging process was working properly, this review process could be relaxed or suspended. If, on the other hand, the FISA court, based on the master’s report, concluded that Americans’ communications were not being properly minimized, the court would have discretion to expand its oversight of this process to insure that the privacy interests of Americans with regard to non-foreign intelligence communications were being protected. There is some similarity between this proposal and the operation of federal wiretaps. Under federal law, “[i]mmediately upon the expiration of the [wiretap order] recordings shall be made available to the judge issuing such order and sealed under his directions.” 18 U.S.C. § 2518(8)(a). This allows the court to assure itself that the government is getting the evidence that the warrant authorized. If the judge concludes that the government was collecting information outside of the scope of the warrant, the FISA court would be able to modify or terminate the wiretap authority or impose any other appropriate restrictions.

The ultimate goal of this would be to align agency practice with statutory and constitutional requirements.

government should be permitted to conduct U.S. person queries so long as the FISA court finds that the U.S. person identifier was reasonably likely to return foreign intelligence information as defined under FISA. If the Board's Recommendation 1 regarding targeting is adopted, the Section 702 program will provide sufficient front-end safeguards that we do not believe a probable cause standard is needed at the query stage. And, provided that the statutory definition of foreign intelligence information is strictly followed, including the requirement that the Americans' information sought be "necessary to" the government's ability to protect against international terrorism or other designated threats, we conclude that it is appropriate for the government to seek such information through U.S. person queries without demonstrating that the American in question is an agent of a foreign power.

At the end, the current system allows a U.S. person about whom there is no suspicion of being a terrorist or engaging in other illegal activity but who unknowingly corresponds with the target of a Section 702 proceeding — perhaps a relative or professional colleague or old friend — to have his or her correspondence with the target, over a period of several years, collected, reviewed at will by intelligence analysts, and retained in a FISA data bank. If the unknowing correspondent's emails or other Internet material do display information of foreign intelligence value, it can be used as such and we have no objection to that. But without any such determination, the correspondence in toto, however private or confidential, can be stored for years and it can be queried using the unknowing correspondent's name as a selector not only by a few but by many NSA foreign intelligence analysts. The unknowing correspondent's information may also be used under restrictions, but nonetheless used and disseminated outside the agency in reports or provided to a foreign government — all this with no prior review beyond that conducted within the intelligence community. The possibility of such an occurrence, even if rare, does not seem to us to come near the Fourth Amendment reasonableness standard for a significant component of Section 702 or to comply with the letter and spirit of FISA. We feel strongly that a neutral and detached judicial officer should approve the use of U.S. person identifiers. That requirement traditionally has been considered a critical component of Fourth Amendment protections against overbroad searches.⁵⁶⁸ As the Supreme Court stated last week, noting the importance of judicial approval for government access to information, "the Founders did not fight a revolution to gain the right to government agency protocols."⁵⁶⁹

⁵⁶⁸ See, e.g., *United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div.*, 407 U.S. 297, 309 (1972) ("*Keith*") (reasonableness under the Fourth Amendment "derives content and meaning through reference to the warrant clause").

⁵⁶⁹ *Riley v. California*, No. 13-132, 2014 WL 2864483, at *16 (U.S. June 25, 2014).

II. Recommendation Regarding FBI Queries for Criminal Purposes

The Board's unanimous Recommendation 2 states that additional limits should be placed on the FBI's use and dissemination of Section 702 data in connection with non-foreign intelligence criminal matters. In our view, these limits should include the requirement that the FBI obtain prior FISA court approval before using identifiers to query Section 702 data to ensure that the identifier is reasonably likely to return information relevant to a criminal assessment or investigation of a crime. In response, Board Members Brand and Cook, in their separate statement, refer to the practice of FBI's using the results of Section 702 data queries in the investigation and prosecution of crimes as largely theoretical. Yet the FBI has not only the capability to conduct such queries but has authorized them, and, in fact, criminal agents do conduct such queries routinely; the fact is that we do not know the precise number of times there is a subsequent use of any results from those queries.⁵⁷⁰

Privacy and civil liberties concerns regarding "incidentally" collected Section 702 information do not just arise when that information is used outside the FBI, such as to obtain a search warrant. The information can also be used inside the FBI to make determinations about Americans that adversely affect them, such as deciding to move from an assessment to a formal criminal investigation. A troubling precedent could be created by permitting a general search of Section 702 material, including incidental collections of innocent Americans' private information, which was collected with no articulable suspicion and particularized judicial approval and target-specific oversight. It could have implications when it comes to general access throughout the government to big data repositories collected for a specific purpose and under specific restrictions by a particular agency. In the case of domestic criminal law enforcement, which currently operates under a painstaking structure with deep roots in the Fourth Amendment and a myriad of particularized statutes and case law, a general permission to search such protected data without any need to demonstrate even an articulable suspicion about the named selector is especially worrisome. Finally, FISA court judges, who are drawn from the ranks of federal district judges and who preside over grand jury proceedings and criminal trials, have extensive experience in evaluating what is or is not relevant evidence in a criminal

⁵⁷⁰ Board Members Brand and Cook are concerned that any justification for a query at an early stage in a criminal investigation will often be unworkable. The alternative, however, is to permit queries of innocent subjects' Section 702 communications without even an articulable suspicion of wrongdoing or terrorist affiliations. We note also that there is nothing to support the assertion that these queries are less "intrusive" of privacy than the other techniques listed in the Attorney General's Domestic Rules as permissible in early stage investigations, i.e., public information, online resources, volunteered information, consent searches and requested information. Federal Bureau of Investigation, Domestic Investigations and Operations Guide, § 5.9.1 (Oct. 15, 2011), *available at* <http://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIIG%209/fbi-domestic-investigations-and-operations-guide-diog-2011-version>.

investigation and our proposal that they be required to do so would not rule out queries essential to an investigation.

We do not anticipate that requiring judicial approval for queries in ordinary crime situations will erect any serious impediment to law enforcement. On the other hand, Board Members Cook and Brand's suggestion that FBI agents be allowed to use Section 702 data without judicial approval not only in the investigative stage but, with approval by Department of Justice officials, as the basis for a warrant or grand jury subpoena, raises the substantial statutory and constitutional questions discussed above.

Our proposal will not ban any queries regarding U.S. persons or others in investigations of either foreign intelligence or domestic crimes, but rather would interpose a time honored protection of approval by a detached judicial officer of government access to Americans' communications. This is the minimal protection that should be afforded to U.S. persons who have done nothing to merit forfeiture of all Fourth Amendment protection to their private papers.

ANNEX B

Separate Statement by Board Members Rachel Brand and Elisebeth Collins Cook

I. The Program is Legal and Effective

We hope that the length of the Board's report and its comprehensive discussion of the legal considerations surrounding the program will not obscure the Board's unanimous bottom-line conclusion: The core Section 702 program is clearly authorized by Congress, reasonable under the Fourth Amendment, and an extremely valuable and effective intelligence tool.

To the extent that the Board had concerns about the program after our thorough review, they focused primarily on two particular aspects to the program's current operation: the practice of searching the database using a U.S. person identifier, and so-called "about" collection, both of which are discussed at length in the Board's report. The Board makes a few targeted recommendations to address concerns raised by these two aspects of the program. We stress that these are *policy*-based recommendations designed to tighten the program's operation and ameliorate the extent to which these aspects of the program could affect the privacy and civil liberties of U.S. persons. We do not view them to be essential to the program's statutory or constitutional validity.

II. Queries of Section 702 Information

The extent to which additional restrictions should apply to agencies' ability to query information collected pursuant to Section 702 using U.S. person identifiers has divided the Board. In the case of the FBI, this issue is intertwined with questions about querying Section 702 information for non-foreign intelligence purposes, the potential use of Section 702 information in criminal proceedings, and longstanding efforts to ensure information sharing within the agency. Specifically, the Board grappled with what to do about the fact that it is theoretically possible for a database query by an FBI analyst in a non-foreign intelligence criminal matter to return Section 702 information and for this information to be further used in the investigation and prosecution of that crime.⁵⁷¹ In addressing this issue, we believe it important to adopt a policy that matches the scope of the problem, can work as a practical matter, and will not unnecessarily impair the government's ability to conduct counterterrorism and other national security-related investigations.

⁵⁷¹ The FBI receives only a small portion of Section 702 information and receives no information collected upstream. See Letter from Deirdre M. Walsh, Director of Legislative Affairs, to Hon. Ron. Wyden, United States Senate (June 27, 2014) (responding to question regarding number of queries using U.S. person identifiers of communications collected under Section 702).

The concern: As discussed at length in the Board’s Report, Section 702 collection differs from traditional electronic surveillance in a few key ways, including a lower standard for collection and the absence of a particularized judicial finding for targeting decisions. Moreover, Section 702 has an explicit foreign intelligence purpose requirement for authorized collection, consistent with the longstanding distinction between foreign intelligence and criminal purposes reflected elsewhere in FISA. Given these factors, our key concerns were the querying of Section 702 collection for *non-foreign intelligence* purposes, and the potential subsequent use of that information to further a non-foreign intelligence criminal investigation or prosecution.⁵⁷²

Scope: According to initial information provided by the FBI, it seems clear that FBI agents and analysts routinely conduct queries across all FBI databases in non-foreign intelligence investigations and assessments. This is unsurprising, given that the FBI has traditionally considered the querying of information already within its possession to be among the least intrusive investigative techniques available, and the agency’s overall efforts since 9/11 to foster information sharing and eliminate stovepipes. But the story is far different for the potential *use* of Section 702 information in the investigation or prosecution of non-foreign intelligence crimes. We are unaware of any instance in which a database query in an investigation of a non-foreign intelligence crime resulted in a “hit” on 702 information, much less a situation in which such information was used to further such an investigation or prosecution.

Our proposal: As stated in the Board’s Report, we would not place limitations on the FBI’s ability to include its FISA database among the databases *queried* in non-foreign intelligence criminal matters. We believe that querying information already in the FBI’s possession is a relatively non-intrusive investigative tool, and the discovery of potential links between ongoing criminal and foreign intelligence investigations is potentially critical to national security.⁵⁷³ Instead, we would require an analyst who has not had FISA training to seek supervisory approval before *viewing* responsive Section 702 information, to ensure that the information continues to be treated consistent with applicable statutory and court-imposed restrictions.

We believe that placing some additional limitations on the *use* of Section 702 information in non-foreign intelligence criminal matters may also be warranted because of the increased civil liberties concerns raised by the use of FISA information outside the foreign intelligence context. Conceptually, the appropriate point at which to potentially limit the use of that information is where it could infringe on a person’s liberty by, for

⁵⁷² See *In re Sealed Case*, 310 F.3d 717 (FISA Ct. Rev. November 18, 2002).

⁵⁷³ See pages 108-10 of this Report. See generally, The Webster Commission, *Final Report of the William H. Webster Commission on the Federal Bureau of Investigation, Counterterrorism Intelligence, and the Events at Fort Hood, Texas, on November 5, 2009* (2012).

example, being used as the basis for obtaining a search warrant, wiretap, or other intrusive investigative tool, as the basis for a criminal indictment in a grand jury proceeding, or as evidence in a criminal prosecution. Where current policy does not already require the approval of at least the Assistant Attorney General,⁵⁷⁴ we would require such approval before Section 702 information could be used in these contexts.

We note that it is already very unlikely that Section 702 information would be used in this way because of the existing significant hurdles to the use of *any* FISA-derived information in a criminal proceeding.⁵⁷⁵ FISA requires the personal approval of the Attorney General, Deputy Attorney General, or Assistant Attorney General for National Security before FISA-derived information can be used as evidence at trial or in some of the more preliminary stages of the criminal process, such as before the grand jury.⁵⁷⁶ FISA also requires that criminal defendants be notified if FISA-derived information will be used against them in a criminal proceeding. And since any decision to use Section 702 information risks revealing the intelligence community's sources and methods, there is always a strong disincentive to permit it. The hurdles imposed by these existing requirements result in Section 702 information being used rarely in the prosecution of even national security-related crimes, and perhaps never in the prosecution of other crimes. As such, our proposal would not create an entirely new and unknown set of rules, but would build an added level of protection for civil liberties into the existing structure.

Concerns with requiring court approval prior to querying: Chairman Medine and Member Wald would require the FBI to obtain FISC approval prior to querying FISA-obtained information, regardless of whether the query relates to a U.S. person, and even in the investigation of foreign intelligence crimes such as terrorism or espionage. For an FBI query for foreign intelligence purposes (not including investigation of foreign intelligence crimes), the FISC would have to first determine that the query was likely to return foreign intelligence information. For an FBI query in the investigation of any crime—including foreign intelligence crimes—the FISC would have to first determine that the query was likely to return evidence relevant to the investigation.⁵⁷⁷ We have significant concerns

⁵⁷⁴ See Memorandum from Michael B. Mukasey, Attorney General, to all Federal Prosecutors, *Revised Policy on the Use or Disclosure of FISA Information*, at 2-7 (January 10, 2008).

⁵⁷⁵ 50 U.S.C. § 1806(b).

⁵⁷⁶ *Id.* at §1806(c). We note that the Department of Justice has recently clarified its view of when information used in a criminal proceeding may be “derived from” prior Title VII FISA collection. See, e.g., *United States v. Mohamud*, No. 3:10-CR-475 slip op. at 3 (D. Or. June 24, 2014) (quoting government filing). In addition, the Department’s FISA Use Policy imposes additional restrictions to the use of Section 702 information in the context of more routine criminal investigative activities.

⁵⁷⁷ Foreign intelligence investigations routinely encompass foreign intelligence crimes. How the FBI or the FISA Court would determine which of these standards applied is unclear.

about the implications of this approach, which would likely have significant detrimental consequences far greater than acknowledged (or perhaps intended) by our colleagues.

First and foremost, although the apparent motivation of this proposal is to protect U.S. persons, it could not be limited to U.S. persons in practice. The FBI (our domestic law enforcement agency) naturally does not distinguish between U.S. persons and non-U.S. persons, which means this proposed requirement would apply by default to *all* queries of the FISA database, by *all* FBI personnel, in *any* FBI investigation of *any* crime. And requiring the FBI to determine whether the subject of a query is a U.S. person could result in more intrusive investigation of that person than would otherwise occur.⁵⁷⁸

Similarly, although the motivation of the proposal is to address incidental collection of U.S. person information through the Section 702 program, the FBI currently combines all FISA-obtained information in one database, which means that as a practical matter the proposal would prohibit the FBI from searching any FISA-obtained information without first obtaining a court order.

Although Chairman Medine and Member Wald reference a requirement for “judicial approval for queries in ordinary crime situations,” the text of their proposal covers even foreign intelligence crimes, meaning that an FBI agent investigating an al Qaeda operative for terrorism would have to go to the FISA court to run a query of any FISA-obtained information. Requiring the FBI to undertake the lengthy and burdensome FISC approval process before an FBI analyst could even query the information would create practical challenges so daunting that it likely never would be pursued. Even if the FBI could obtain prior approval, this would result in significant delay of the investigation and potentially enormous burdens on the FISC. The practical effect of this proposal would be to prevent the FBI from using one of our most valuable foreign intelligence tools to investigate foreign intelligence crimes. It is hard to imagine adopting a rule that is so at odds with the recommendations of the 9/11 Commission, the Webster Commission, and others in the years following 9/11.⁵⁷⁹

In addition to requiring judicial approval, the proposal would impose a standard for the court’s approval in investigations of crime that would be unworkable in many circumstances. Database queries are often used at the earliest stages of an investigation – such as during an assessment, perhaps to follow up on a tip. At this stage, an analyst knows very little and conducts a query to see if there is anything at all that creates a reason to

⁵⁷⁸ Although apparently grounded in Fourth Amendment principles, the proposal makes no distinctions between contents of communications and metadata—as to which there is *no* currently recognized Fourth Amendment interest.

⁵⁷⁹ See National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*, at 78-80, 416-418 (2004); *The Webster Commission Report*, at 94-95 and 136-39.

further pursue the investigation. It is hard to imagine the basis on which the FISC could assess what, if anything, will be returned in a database query at this stage, which would require the FISC to deny the application.

Finally, the proposal could actually exacerbate civil liberties concerns in at least two respects. First, a query of information already in the FBI's possession has been considered one of the least intrusive investigative means available, and is therefore one of the first steps taken in any assessment or investigation. But now in order to use this preliminary investigative tool, our colleagues would require the FBI to assemble information sufficient to facilitate meaningful judicial review, which will inevitably require the use of *more* intrusive means. Second, because queries at the early stages of an investigation are often used to eliminate individuals from suspicion, discouraging queries could prevent the discovery of exculpatory information that otherwise might establish an individual's innocence.

NSA and CIA: Our colleagues also would require prior court approval for NSA and CIA queries of Section 702 information when they involve U.S. person identifiers. Based on our review of the current use and extensive oversight of U.S. Person queries at the NSA and CIA, which we have accurately characterized at "rigorous,"⁵⁸⁰ the majority has declined to recommend such a requirement.⁵⁸¹

⁵⁸⁰ Board Report at Recommendation 4.

⁵⁸¹ We are also concerned about the potential implications of Chairman Medine and Member Wald's proposal regarding minimization. To the extent that their approach requires an analyst to review U.S. Person communications that the analyst would not otherwise review, we think it far from clear that it is more protective of privacy than leaving those communications in the database unreviewed until the end of the retention period.

ANNEX C

AGENDA OF PUBLIC WORKSHOP

HELD ON JULY 9, 2013

Link to Workshop transcript:

<http://www.pclob.gov/All%20Documents/July%209,%202013%20Workshop%20Transcript.pdf>



PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

Workshop Regarding Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act

July 9, 2013

**Renaissance Mayflower Hotel – Grand Ballroom
1127 Connecticut Ave NW, Washington DC**

AGENDA

- 09:00** **Doors Open**
- 09:30 – 09:45** **Introductory Remarks (David Medine, PCLOB Chairman)**
- 09:45 – 11:30** **Panel I: Legal/Constitutional Perspective**
Facilitators: Rachel Brand and Patricia Wald, Board Members
- Panel Members:**
- **Steven Bradbury (Formerly DOJ Office of Legal Counsel)**
 - **Jameel Jaffer (ACLU)**
 - **Kate Martin (Center for National Security Studies)**
 - **Hon. James Robertson, Ret. (formerly District Court and Foreign Intelligence Surveillance Court)**
 - **Kenneth Wainstein (formerly DOJ National Security Division/ White House Homeland Security Advisor)**
- 12:30 – 2:00** **Panel II: Role of Technology**
Facilitators: James Dempsey and David Medine, Board Members
- Panel Members:**
- **Steven Bellovin (Columbia University Computer Science Department)**
 - **Marc Rotenberg (Electronic Privacy Information Center)**

- **Ashkan Soltani (Independent Researcher and Consultant)**
- **Daniel Weitzner (MIT Computer Science and Artificial Intelligence Lab)**

2:00 – 2:15 Break

2:15 – 4:00 Panel III: Policy Perspective
Facilitators: Elisebeth Collins Cook and David Medine, Board Members

Panel Members:

- **James Baker (formerly DOJ Office of Intelligence and Policy Review)**
- **Michael Davidson (formerly Senate Legal Counsel)**
- **Sharon Bradford Franklin (The Constitution Project)**
- **Elizabeth Goitein (Brennan Center for Justice)**
- **Greg Nojeim (Center for Democracy and Technology)**
- **Nathan Sales (George Mason School of Law)**

4:00 – 4:10 Break

4:10 – 4:30 Open for Public Comment

4:30 Closing Comments (David Medine, PCLOB Chairman)

Affiliations are listed for identification purposes only.

ANNEX D

AGENDA OF PUBLIC HEARING

HELD ON NOVEMBER 4, 2013

Link to Hearing transcript:

<http://www.pclob.gov/SiteAssets/PCLOB%20Hearing%20-%20Full%20Day%20transcript%20Nov%204%202013.pdf>



**PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD
PUBLIC HEARING**

*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
November 4, 2013*

**Renaissance Mayflower Hotel – Grand Ballroom
1127 Connecticut Ave NW, Washington DC**

AGENDA

- 08:45** **Doors Open**
- 09:15 – 09:30** **Introductory Remarks (David Medine, PCLOB Chairman, with Board Members Rachel Brand, Elisebeth Collins Cook, James Dempsey, and Patricia Wald)**
- 09:30 – 11:45** **Panel I: Section 215 USA PATRIOT Act and Section 702 Foreign Intelligence Surveillance Act**
- **Rajesh De (General Counsel, National Security Agency)**
 - **Patrick Kelley (Acting General Counsel, Federal Bureau of Investigation)**
 - **Robert Litt (General Counsel, Office of the Director of National Intelligence)**
 - **Brad Wiegmann (Deputy Assistant Attorney General, National Security Division, Department of Justice)**
- 11:45 – 1:15** **Lunch Break (on your own)**
- 1:15 – 2:30** **Panel II: Foreign Intelligence Surveillance Court**

- **James A. Baker (formerly DOJ Office of Intelligence and Policy Review)**
- **Judge James Carr (Senior Federal Judge, U.S. District Court, Northern District of Ohio and former FISA Court Judge 2002-2008)**
- **Marc Zwillinger (Founder, ZwillGen PLLC and former Department of Justice Attorney, Computer Crime & Intellectual Property Section)**

2:30 – 2:45 Break

2:45 – 4:15 Panel III: Academics and Outside Experts

- **Jane Harman (Director, President and CEO, The Woodrow Wilson Center and former Member of Congress)**
- **Orin Kerr (Fred C. Stevenson Research Professor, George Washington University Law School)**
- **Stephanie K. Pell (Principal, SKP Strategies, LLC; former House Judiciary Committee Counsel and Federal Prosecutor)**
- **Eugene Spafford (Professor of Computer Science and Executive Director, Center for Education and Research in Information Assurance and Security, Perdue University)**
- **Stephen Vladeck (Professor of Law and the Associate Dean for Scholarship at American University Washington College of Law)**

4:15 Closing Comments (David Medine, PLCOB Chairman)

All Affiliations are listed for identification purposes only.

ANNEX E

AGENDA OF PUBLIC HEARING

HELD ON March 19, 2014

Link to Hearing transcript:

http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/19-March-2014_Public_Hearing_Transcript.pdf



**PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD
PUBLIC HEARING**

***Hearing Regarding the Surveillance Program Operated Pursuant
Section 702 of the Foreign Intelligence Surveillance Act***

March 19, 2014

**Renaissance Mayflower Hotel – Grand Ballroom
1127 Connecticut Ave NW, Washington DC**

AGENDA

08:45 Doors Open

**09:00 - 09:10 Introductory Remarks (David Medine, PCLOB Chairman)
Panel I: Government Perspective on Section 702 Foreign
Intelligence Surveillance Act**

Panelists:

09:15 - 10:45

- **James A. Baker (General Counsel, Federal Bureau of Investigation)**
- **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)**

**10:45 - 11:00 Break
Panel II: Legal Issues with 702 Foreign Intelligence Surveillance
Act**

11:00 - 12:30 *Panelists:*

- **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)**

**12:30 - 1:45 Lunch Break (on your own)
Panel III: Transnational and Policy Issues**

Panelists:

- **John Bellinger (Partner, Arnold & Porter)**
- **Dean C. Garfield (President and CEO, Information Technology Industry Council)**
- **Laura Pitter (Senior National Security Researcher, Human Rights Watch)**
- **Eric Posner (Professor of Law, University of Chicago Law School)**
- **Ulrich Sieber (Director, Max Planck Institute for Foreign and International Criminal Law, Freiburg/Germany)**
- **Christopher Wolf (Partner, Hogan Lovells)**

3:45 Closing Comments (David Medine, PCLOB Chairman)

All Affiliations are listed for identification purposes only.

ANNEX F

Request for Public Comments on Board Study

The Federal Register

The Daily Journal of the United States Government

56952 Federal Register/Vol. 78, No. 179/Monday, September 16, 2013/Notices
PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

[Notice-PCLOB-2013-06; Docket No. 2013- 0005; Sequence No. 6]

Notice of Hearing

A Notice by the Privacy and Civil Liberties Oversight Board on 10/25/2013

Action

Notice Of A Hearing.

Summary

The Privacy and Civil Liberties Oversight Board (PCLOB) will conduct a public hearing with current and former government officials and others to address the activities and responsibilities of the executive and judicial branches of the federal government regarding the government's counterterrorism surveillance programs. This hearing will continue the PCLOB's study of the federal government's surveillance programs operated pursuant to Section 215 of the USA PATRIOT Act and Section 702 of Foreign Intelligence Surveillance Act. Recommendations for changes to these programs and the operations of the Foreign Intelligence Surveillance Court will be considered at the hearing to ensure that counterterrorism efforts properly balance the need to protect privacy and civil liberties. Visit www.pclob.gov for the full agenda closer to the hearing date. This hearing was re-scheduled from October 4, 2013, due to the unavailability of witnesses as a result of the federal lapse in appropriations.

DATES:

Monday, November 4, 2013; 9:00 a.m.-4:30 p.m. (Eastern Standard Time).

Comments:

You may submit comments with the docket number PCLOB-2013-0005; Sequence 7 by the following method:

- *Federal eRulemaking Portal*: Go to <http://www.regulations.gov>. Follow the on-line instructions for submitting comments.
- Written comments may be submitted at any time prior to the closing of the docket at 11:59 p.m. Eastern Time on November 14, 2013. This comment period has been extended from October 25, 2013, as a result of the new hearing date.

All comments will be made publicly available and posted without change. Do not include personal or confidential information.

ADDRESSES:

Mayflower Renaissance Hotel Washington, 1127 Connecticut Ave. NW., Washington DC 20036. Facility's location is near Farragut North Metro station.

FOR FURTHER INFORMATION CONTACT:

Susan Reingold, Chief Administrative Officer, 202-331-1986. For email inquiries, please email info@pclob.gov.

SUPPLEMENTARY INFORMATION:

Procedures for Public Participation

The hearing will be open to the public. Individuals who plan to attend and require special assistance, such as sign language interpretation or other reasonable accommodations, should contact Susan Reingold, Chief Administrative Officer, 202-331-1986, at least 72 hours prior to the meeting date.

Dated: October 21, 2013.

Diane Janosek,
Chief Legal Officer, Privacy and Civil Liberties Oversight Board.

<https://www.federalregister.gov/articles/2013/10/25/2013-25103/notice-of-hearing>

ANNEX G

Reopening the Public Comment Period

At the March 19, 2014 public hearing, the Privacy and Civil Liberties Oversight Board (PCLOB) Chairman announced the reopening of the public comment period to allow for additional submissions in light of the information discussed and submitted during the March 19, 2014 public hearing. All comments received were posted to the PCLOB Docket No. 2013-005 and can be viewed at <http://www.regulations.gov/#!docketDetail;D=PCLOB-2013-0005>.

ANNEX H

**Index to Public Comments received to PCLOB Docket No. 2013-005 on
www.regulations.gov.**

Comments Received on PCLOB Docket No. 2013-005

Can also view all entries at: <http://www.regulations.gov/#!docketDetail;D=PCLOB-2013-0005>

Entity submitting comment - listed in order as they appear on docket	Go to URL to see comment on Docket	Additional details:
Global Network Initiative (GNI)	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0027	GNI is a multi-stakeholder group of companies, civil society organizations (including human rights and press freedom groups), investors and academics
Private individual	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0044	
Nathan Sales	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0022	Panel member at PCLOB Workshop

European Digital Rights (EDRi) and the Fundamental Rights European Experts Group (FREE)	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0024	EDRi is an association of 35 digital civil rights organizations from 21 European countries. FREE is an association whose focus is on monitoring, teaching and advocating in the EU.
Michael Davidson	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0020	Panel member at PCLOB Workshop
Project On Government Oversight (POGO), National Security Counselors, and OpenTheGovernment.org	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0029	
Center for National Security Studies	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0033	

Michael Davidson-second submission	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0028	Providing the July 30th opinion of the U.S. Court of Appeals for the Fifth Circuit in In re: Application of the United States of America for Historical Cell Site Data, No. 11-20884
Mr Juan Fernando López Aguilar, Chair of the European Parliament's Civil Liberties, Justice and Home Affairs Committee	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0059	
Ashkan Soltani	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0023	Panel member at PCLOB Workshop
Alliance for Justice	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0035	
Alan Charles Raul	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0065	Has four attachments
“Three former intelligence professionals - all former employees of the National Security Agency”	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0053	Statement submitted
Private citizen anonymous	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0014	

Coalition of 53 groups- letter	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0038	This is an updated coalition letter to PCLOB
The Constitution Project	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0009	Sharon Bradford Franklin was Panel member at PCLOB Workshop
Computer and Communications Industry Association	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0025	
Private citizen anonymous	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0017	
Electronic Frontier Foundation	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0030	
BSA /The Software Alliance Computer & Communications Industry Association (CCIA)/ Information Technology Industry Council (ITI)/ SIIA (Software & Information Industry Association)/ TechNet	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0061	

Ashkan Soltani	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0039	Revised submission, was a panel member at PCLOB Workshop
Private citizen anonymous	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0005	
Daniel J. Weitzner, Massachusetts Institute of Technology	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0040	Panel member at PCLOB Workshop
Private citizen anonymous	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0052	
Access - AccessNow.org	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0048	
Information and Privacy Commissioner of Ontario, Canada, Dr. Ann Cavoukian	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0057	
Privacy Times	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0011	
Electronic Privacy Information Center	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0064	Marc Rotenberg was a panel member at PCLOB Workshop

ACLU Statement	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0032	Jameel Jaffer was a panel member at PCLOB Workshop and Hearing
Private citizen anonymous	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0046	
Mark Sokolow	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0018	
GodlyGlobal.org	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0019	A faith-based initiative based in Switzerland with global scope
Private citizen anonymous	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0041	
ACCESS NOW	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0047	Second posting
Coalition letter	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0010	
Center for Democracy & Technology, Gregory T. Nojeim	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0034	Gregory Nojeim was a panel member at PCLOB Workshop
Reporters Committee for Freedom of the Press	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0063	

Center for National Security Studies	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0060	
Private citizen anonymous	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0037	
Brennan Center for Justice's Liberty and National Security Program	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0049	Elizabeth Goitein was a panel member at PCLOB Workshop
Jeffrey H. Collins	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0043	
Jeffrey H. Collins	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0045	Amended
Steven G. Bradbury	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0012	Panel member at PCLOB Workshop
Human Rights Watch	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0036	
"Human rights organizations and advocates from around the world"	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0042	Dozens of countries represented

Steven M. Bellovin	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0021	Panel member at PCLOB Workshop
Board of the U.S. Public Policy Council of the Association for Computing Machinery	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0026	Eugene H. Spafford was a panel member at PCLOB Hearing
Private citizen	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0066	
Caspar Bowden, Prepared for the European Parliament LIBE Committee	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0068	
Stephanie Pell	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0069	Panel member at PCLOB hearing
Congressman Bennie Thompson	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0071	Ranking Member, Committee on Homeland Security
Government Accountability Project	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0072	
Jennifer S. Granick	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0090	
Private citizen anonymous	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0007	

Information Technology Industry Council	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0074	
Stephanie Pell	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0070	Panel member at PCLOB hearing
BSA The Software Alliance, Computer & Communications Industry Association (CCIA), Information Technology Industry Council (ITI), SIIA - Software & Information Industry Association, TechNet	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0067	
Jameel Jaffer	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0082	Panel member at PCLOB workshop and hearing
Government Accountability Project	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0083	
Martin Scheinin	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0085	Panel member at PCLOB hearing
Marshall Erwin	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0089	
Electronic Frontier Foundation	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0100	

Christopher Wolf	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0087	Panel member at PCLOB hearing
Thomas Drake	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0102	Panel member at PCLOB hearing
Laura Pitter	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0079	Panel member at PCLOB hearing
NSA Director of Civil Liberties and Privacy Office Report on NSA's Implementation of FISA Section 702	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0101	
Laura K. Donohue	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0075	Panel member at PCLOB hearing
Julian G. Ku	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0086	Panel member at PCLOB hearing
PEN American Center	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0094	
Eric A. Posner	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0081	Panel member at PCLOB hearing
Hogan Lovell	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0088	
National Association of Criminal Defense Lawyers	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0091	

Ben Davis	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0084	
Amnesty International USA and the American Civil Liberties Union	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0096	
Brennan Center for Justice	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0093	
Christopher Wolf	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0078	Panel member at PCLOB hearing
Kevin Cahill	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0105	
The Constitution Project	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0099	
Center for Democracy & Technology	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0095	
Dean C. Garfield	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0077	Panel member at PCLOB hearing
Laura Donohue	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0104	Panel member at PCLOB hearing
Center for National Security Studies	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0098	
John B. Bellinger, III	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0076	Panel member at PCLOB hearing

William Binney, Thomas Drake, Edward Loomis, J. Kirk Wiebe, Ray McGovern, Elizabeth Murray, Coleen Rowley, Daniel Ellsberg	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0103	
Rachel Levinson- Waldman	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0080	Panel member at PCLOB hearing
Center for Democracy and Technology, Center for National Security Studies, National Association of Criminal Defense Lawyers, OpenTheGovernment .Org, The Constitution Project	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0106	

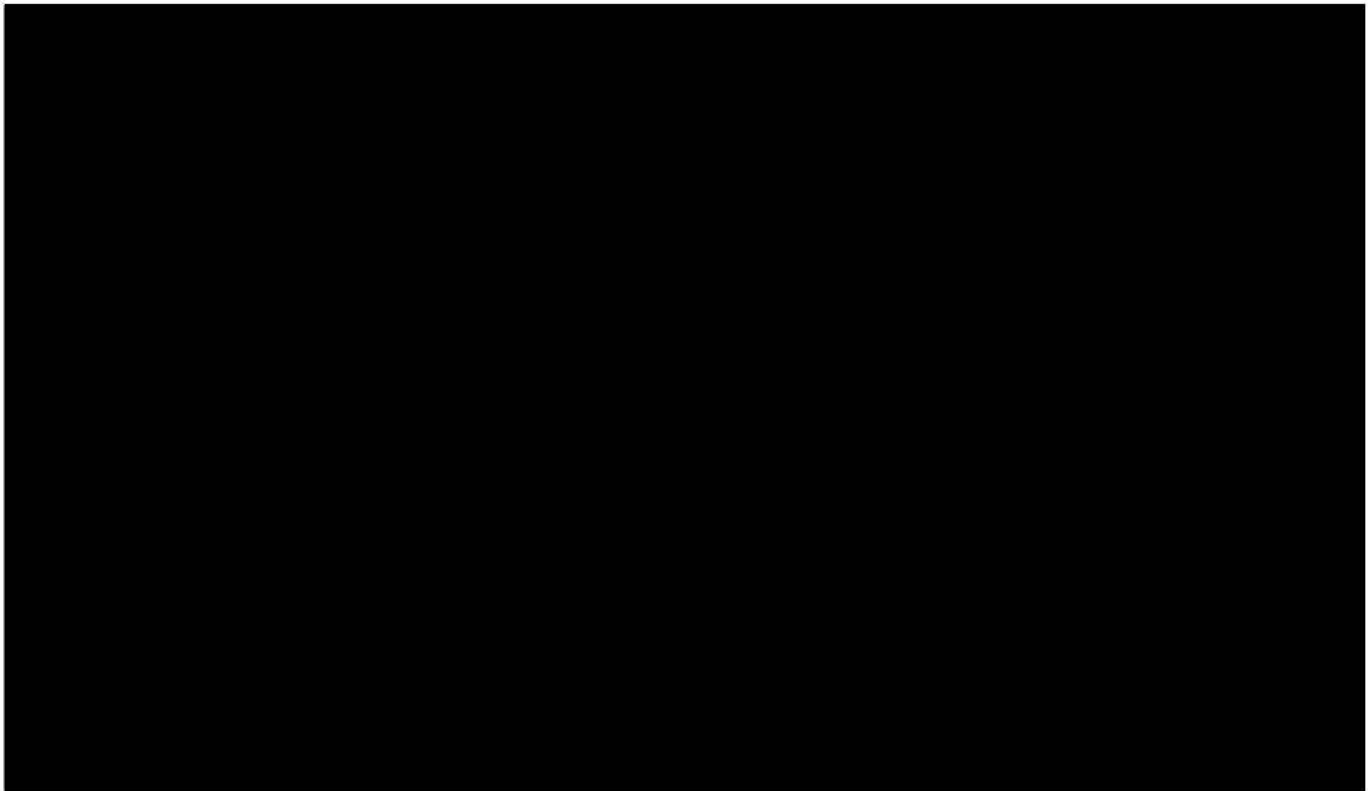
This Report is the Privacy and Civil Liberties Oversight Board's effort to analyze and review actions the executive branch takes to protect the Nation from terrorism to ensure the proper balancing of these actions with privacy and civil liberties.

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 16

~~TOP SECRET//COMINT//ORCON,NOFORN~~

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.



MEMORANDUM OPINION

These matters are before the Foreign Intelligence Surveillance Court (“FISC” or “Court”) on: (1) the “Government’s Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications” for DNI/AG 702(g) Certifications

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

[REDACTED], which was filed on April 20, 2011; (2) the “Government’s Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications” for DNI/AG 702(g) Certifications [REDACTED], which was filed on April 22, 2011; and (3) the “Government’s Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications” for DNI/AG 702(g) Certifications [REDACTED], which was also filed on April 22, 2011.¹

Through these submissions, the government seeks approval of the acquisition of certain telephone and Internet communications pursuant to Section 702 of the Foreign Intelligence Surveillance Act (“FISA” or the “Act”), 50 U.S.C. § 1881a, which requires judicial review for compliance with both statutory and constitutional requirements. For the reasons set forth below, the government’s requests for approval are granted in part and denied in part. The Court concludes that one aspect of the proposed collection – the “upstream collection” of Internet transactions containing multiple communications – is, in some respects, deficient on statutory and constitutional grounds.

¹ For ease of reference, the Court will refer to these three filings collectively as the “April 2011 Submissions.”

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

I. BACKGROUND

A. The Certifications and Amendments

The April 2011 Submissions include DNI/AG 702(g) Certification [REDACTED]

[REDACTED], all of which were executed by the Attorney General and the Director of National Intelligence (“DNI”) pursuant to Section 702. [REDACTED] previous certifications have been submitted by the government and approved by the Court pursuant to Section 702. [REDACTED]

[REDACTED] (collectively, the “Prior 702 Dockets”). Each of the April 2011 Submissions also includes supporting affidavits by the Director or Acting Director of the National Security Agency (“NSA”), the Director of the Federal Bureau of Investigation (“FBI”), and the Director of the Central Intelligence Agency (“CIA”); two sets of targeting procedures, for use by NSA and FBI respectively; and three sets of minimization procedures, for use by NSA, FBI, and CIA, respectively.²

Like the acquisitions approved by the Court in the eight Prior 702 Dockets, collection

² The targeting and minimization procedures accompanying Certification [REDACTED] are identical to those accompanying [REDACTED]. As discussed below, the NSA targeting procedures and FBI minimization procedures accompanying Certifications [REDACTED] also are identical to the NSA targeting procedures and FBI minimization procedures that were submitted by the government and approved by the Court for use in connection with Certifications [REDACTED]. The FBI targeting procedures and the NSA and CIA minimization procedures that accompany the April 2011 Submissions differ in several respects from the corresponding procedures that were submitted by the government and approved by the Court in connection with Certifications [REDACTED].

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

under Certifications [REDACTED] is limited to “the targeting of non-United States persons reasonably believed to be located outside the United States.” Certification [REDACTED]

[REDACTED]

The April 2011 Submissions also include amendments to certifications that have been submitted by the government and approved by the Court in the Prior 702 Dockets. The amendments, which have been authorized by the Attorney General and the DNI, provide that information collected under the certifications in the Prior 702 Dockets will, effective upon the Court’s approval of Certifications [REDACTED], be handled subject to the same

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

revised NSA and CIA minimization procedures that have been submitted for use in connection with Certifications [REDACTED]

[REDACTED]

B. The May 2 “Clarification” Letter

On May 2, 2011, the government filed with the Court a letter pursuant to FISC Rule 13(a) titled “Clarification of National Security Agency’s Upstream Collection Pursuant to Section 702 of FISA” (“May 2 Letter”). The May 2 Letter disclosed to the Court for the first time that NSA’s “upstream collection”³ of Internet communications includes the acquisition of entire

“transaction[s]” (b) (1) (A) [REDACTED]

[REDACTED]⁴ According to the May 2 Letter, such transactions may contain data that is wholly unrelated to the tasked selector, including the full content of discrete communications that are not to, from, or about the facility tasked for collection. See id. at 2-3. The letter noted that NSA uses [REDACTED] to ensure that “the person from whom it seeks to obtain foreign intelligence information is located overseas,” but suggested that the government might lack confidence in the effectiveness of such measures as applied to Internet transactions. See id. at 3 (citation omitted).

³ The term “upstream collection” refers to NSA’s interception of Internet communications as they transit (b) (1) (A) [REDACTED], rather than to acquisitions directly from Internet service providers such as [REDACTED]. [REDACTED]

⁴ The concept of “Internet transactions” is discussed more fully below. See infra, pages 27-41 and note 23.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

C. The Government's First Motion for Extensions of Time

On May 5, 2011, the government filed a motion seeking to extend until July 22, 2011, the 30-day periods in which the Court must otherwise complete its review of Certifications [REDACTED], and the amendments to the certifications in the Prior 702 Dockets. See Motion for an Order Extending Time Limit Pursuant to 50 U.S.C. § 1881a(j)(2) at 1 (“May Motion”). The period for FISC review of Certification [REDACTED] was then set to expire on May 20, 2011, and the period for review of the other pending certifications and amendments was set to expire on May 22, 2011. Id. at 6.⁵

The government noted in the May Motion that its efforts to address the issues raised in the May 2 Letter were still ongoing and that it intended to “supplement the record . . . in a manner that will aid the Court in its review” of the certifications and amendments and in making the determinations required under Section 702. Id. at 7. According to the May Motion, however, the government would “not be in a position to supplement the record until after the statutory time limits for such review have expired.” Id. The government further asserted that granting the requested extension of time would be consistent with national security, because, by operation of

⁵ 50 U.S.C. § 1881a(i)(1)(B) requires the Court to complete its review of the certification and accompanying targeting and minimization procedures and issue an order under subsection 1881a(i)(3) not later than 30 days after the date on which the certification and procedures are submitted. Pursuant to subsection 1881a(i)(1)(C), the same time limit applies to review of an amended certification or amended procedures. However, 50 U.S.C. § 1881a(j)(2) permits the Court, by order for reasons stated, to extend “as necessary for good cause in a manner consistent with national security,” the time limit for the Court to complete its review and issue an order under Section 1881a(i)(3).

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

statute, the government's acquisition of foreign intelligence information under Certifications

[REDACTED] could continue pending completion of the Court's review. See id. at 9-10.

On May 9, 2011, the Court entered orders granting the government's May Motion. Based upon the representations in the motion, the Court found that there was good cause to extend the time limit for its review of the certifications to July 22, 2011, and that the extensions were consistent with national security. May 9, 2011 Orders at 4.

D. The May 9 Briefing Order

Because it appeared to the Court that the acquisitions described in the May 2 Letter exceeded the scope of collection previously disclosed by the government and approved by the Court, and might, in part, fall outside the scope of Section 702, the Court issued a Briefing Order on May 9, 2011 ("Briefing Order"), in which it directed the government to answer a number of questions in writing. Briefing Order at 3-5. On June 1, 2011, the United States filed the "Government's Response to the Court's Briefing Order of May 9, 2011" ("June 1 Submission"). After reviewing the June 1 Submission, the Court, through its staff, directed the government to answer a number of follow-up questions. On June 28, 2011, the government submitted its written responses to the Court's follow-up questions in the "Government's Response to the Court's Follow-Up Questions of June 17, 2011" ("June 28 Submission").

E. The Government's Second Motion for Extensions of Time

The Court met with senior officials of the Department of Justice on July 8, 2011, to

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

discuss the information provided by the government in the June 1 and June 28 Submissions. During the meeting, the Court informed the government that it still had serious concerns regarding NSA's acquisition of Internet transactions and, in particular, whether the Court could make the findings necessary to approve the acquisition of such transactions pursuant to Section 702. The Court also noted its willingness to entertain any additional filings that the government might choose to make in an effort to address those concerns.

On July 14, 2011, the government filed a motion seeking additional sixty-day extensions of the periods in which the Court must complete its review of DNI/AG 702(g) Certifications [REDACTED], and the amendments to the certifications in the Prior 702 Dockets. Motion for Orders Extending Time Limits Pursuant to 50 U.S.C. § 1881a(j)(2) ("July Motion").⁶

In its July Motion, the government indicated that it was in the process of compiling additional information regarding the nature and scope of NSA's upstream collection, and that it was "examining whether enhancements to NSA's systems or processes could be made to further ensure that information acquired through NSA's upstream collection is handled in accordance with the requirements of the Act." *Id.* at 8. Because additional time would be needed to supplement the record, however, the government represented that a 60-day extension would be necessary. *Id.* at 8, 11. The government argued that granting the request for an additional extension of time would be consistent with national security, because, by operation of statute, the

⁶ As discussed above, by operation of the Court's order of May 9, 2011, pursuant to 50 U.S.C. § 1881a(j)(2), the Court was required to complete its review of, and issue orders under 50 U.S.C. § 1881a(i)(3) concerning, DNI/AG 702(g) Certifications [REDACTED] and the amendments to the certifications in the Prior 702 Dockets, by July 22, 2011. *Id.* at 6.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

government's acquisition of foreign intelligence information under Certifications [REDACTED]

[REDACTED] could continue pending completion of the Court's review. *Id.* at 9-10.

On July 14, 2011, the Court entered orders granting the government's motion. Based upon the representations in the motion, the Court found that there was good cause to extend the time limit for its review of the certifications to September 20, 2011, and that the extensions were consistent with national security. July 14, 2011 Orders at 4.

F. The August 16 and August 30 Submissions

On August 16, 2011, the government filed a supplement to the June 1 and June 28 Submissions ("August 16 Submission"). In the August 16 Submission, the government described the results of "a manual review by [NSA] of a statistically representative sample of the nature and scope of the Internet communications acquired through NSA's . . . Section 702 upstream collection during a six-month period." Notice of Filing of Aug. 16 Submission at 2. Following a meeting between the Court staff and representatives of the Department of Justice on August 22, 2011, the government submitted a further filing on August 30, 2011 ("August 30 Submission").

G. The Hearing and the Government's Final Written Submission

Following review of the August 30 Submission, the Court held a hearing on September 7, 2011, to ask additional questions of NSA and the Department of Justice regarding the government's statistical analysis and the implications of that analysis. The government made its

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

final written submissions on September 9, 2011, and September 13, 2011 (“September 9 Submission” and “September 13 Submission,” respectively).

H. The Final Extension of Time

On September 14, 2011, the Court entered orders further extending the deadline for its completion of the review of the certifications and amendments filed as part of the April Submissions. The Court explained that “[g]iven the complexity of the issues presented in these matters coupled with the Court’s need to fully analyze the supplemental information provided by the government in recent filings, the last of which was submitted to the Court on September 13, 2011, the Court will not be able to complete its review of, and issue orders . . . concerning [the certifications and amendments] by September 20, 2011.” [REDACTED]

[REDACTED] The Court further explained that although it had originally intended to extend the deadline by only one week, the government had advised the Court that “for technical reasons, such a brief extension would compromise the government’s ability to ensure a seamless transition from one Certification to the next.” [REDACTED]

[REDACTED] Accordingly, the Court extended the deadline to October 10, 2011. [REDACTED]

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

II. REVIEW OF CERTIFICATIONS [REDACTED]

The Court must review a certification submitted pursuant to Section 702 of FISA “to determine whether [it] contains all the required elements.” 50 U.S.C. § 1881a(i)(2)(A). The Court’s examination of Certifications [REDACTED] confirms that:

- (1) the certifications have been made under oath by the Attorney General and the DNI, as required by 50 U.S.C. § 1881a(g)(1)(A), see Certification [REDACTED];
- (2) the certifications contain each of the attestations required by 50 U.S.C. § 1881a(g)(2)(A), see Certification [REDACTED];
- (3) as required by 50 U.S.C. § 1881a(g)(2)(B), each of the certifications is accompanied by the applicable targeting procedures⁷ and minimization procedures;⁸
- (4) each of the certifications is supported by the affidavits of appropriate national security officials, as described in 50 U.S.C. § 1881a(g)(2)(C),⁹ and
- (5) each of the certifications includes an effective date for the authorization in compliance

⁷ See April 2011 Submissions, NSA Targeting Procedures and FBI Targeting Procedures (attached to Certifications [REDACTED]).

⁸ See April 2011 Submissions, NSA Minimization Procedures, FBI Minimization Procedures, and CIA Minimization Procedures (attached to Certifications [REDACTED]).

⁹ See April 2011 Submissions, Affidavits of John C. Inglis, Acting Director, NSA (attached to Certifications [REDACTED]); Affidavit of Gen. Keith B. Alexander, U.S. Army, Director, NSA (attached to Certification [REDACTED]); Affidavits of Robert S. Mueller, III, Director, FBI (attached to Certifications [REDACTED]); Affidavits of Leon E. Panetta, Director, CIA [REDACTED].

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

with 50 U.S.C. § 1881a(g)(2)(D), see Certification [REDACTED]
[REDACTED].¹⁰

The Court therefore finds that Certification [REDACTED]

[REDACTED] contain all the required elements. 50 U.S.C. § 1881a(i)(2)(A).

III. REVIEW OF THE AMENDMENTS TO THE CERTIFICATIONS IN THE PRIOR DOCKETS.

Under the judicial review procedures that apply to amendments by virtue of Section 1881a(i)(1)(C), the Court must review each of the amended certifications “to determine whether the certification contains all the required elements.” 50 U.S.C. § 1881a(i)(2)(A). The Court has previously determined that the certifications in each of the Prior 702 Dockets, as originally submitted to the Court and previously amended, contained all the required elements.¹¹ Like the prior certifications and amendments, the amendments now before the Court were executed under oath by the Attorney General and the DNI, as required by 50 U.S.C. § 1881a(g)(1)(A), and submitted to the Court within the time allowed under 50 U.S.C. § 1881a(i)(1)(C). See

¹⁰ The statement described in 50 U.S.C. § 1881a(g)(2)(E) is not required in this case because there has been no “exigent circumstances” determination under Section 1881a(c)(2).

¹¹ [REDACTED]

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Certification [REDACTED]¹² Pursuant to Section 1881a(g)(2)(A)(ii), the latest amendments include the attestations of the Attorney General and the DNI that the accompanying NSA and CIA minimization procedures meet the statutory definition of minimization procedures, are consistent with the requirements of the Fourth Amendment, and will be submitted to the Court for approval. Certification [REDACTED] [REDACTED]. The latest amendments also include effective dates that comply with 50 U.S.C. § 1881a(g)(2)(D) and § 1881a(i)(1).

Certification [REDACTED] All other aspects of the certifications in the Prior 702 Dockets – including the further attestations made therein in accordance with § 1881a(g)(2)(A), the NSA targeting procedures and FBI minimization procedures submitted therewith in accordance with § 1881a(g)(2)(B),¹³ and the affidavits executed in support thereof in accordance with § 1881a(g)(2)(C) – are unaltered by the latest amendments.

In light of the foregoing, the Court finds that the certifications in the Prior 702 Dockets, as amended, each contain all the required elements. 50 U.S.C. § 1881a(i)(2)(A).

¹² The amendments to the certifications in the Prior 702 Dockets were approved by the Attorney General on April 11, 2011, and by the DNI on April 13, 2011. See Certification [REDACTED] [REDACTED]

¹³ Of course, targeting under the certifications filed in the Prior 702 Dockets will no longer be permitted following the Court's issuance of an order on Certifications [REDACTED] [REDACTED]

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

IV. REVIEW OF THE TARGETING AND MINIMIZATION PROCEDURES

The Court is required to review the targeting and minimization procedures to determine whether they are consistent with the requirements of 50 U.S.C. § 1881a(d)(1) and (e)(1). See 50 U.S.C. § 1881a(i)(2)(B) and (C); see also 50 U.S.C. § 1881a(i)(1)(C) (providing that amended procedures must be reviewed under the same standard). Section 1881a(d)(1) provides that the targeting procedures must be “reasonably designed” to “ensure that any acquisition authorized under [the certification] 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.” Section 1881a(e)(1) requires that the minimization procedures “meet the definition of minimization procedures under [50 U.S.C. §§] 1801(h) or 1821(4)” Most notably, that definition requires “specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular [surveillance or physical search], 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.” 50 U.S.C. §§ 1801(h) & 1821(4). Finally, the Court must determine whether the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment. 50 U.S.C. § 1881a(i)(3)(A).

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

A. The Effect of the Government's Disclosures Regarding NSA's Acquisition of Internet Transactions on the Court's Review of the Targeting and Minimization Procedures

The Court's review of the targeting and minimization procedures submitted with the April 2011 Submissions is complicated by the government's recent revelation that NSA's acquisition of Internet communications through its upstream collection under Section 702 is accomplished by acquiring Internet "transactions," which may contain a single, discrete communication, or multiple discrete communications, including communications that are neither to, from, nor about targeted facilities. June 1 Submission at 1-2. That revelation fundamentally alters the Court's understanding of the scope of the collection conducted pursuant to Section 702 and requires careful reexamination of many of the assessments and presumptions underlying its prior approvals.

In the first Section 702 docket, [REDACTED], the government disclosed that its Section 702 collection would include both telephone and Internet communications. According to the government, the acquisition of telephonic communications would be limited to "to/from" communications – *i.e.*, communications to or from a tasked facility. The government explained, however, that the Internet communications acquired would include both to/from communications and "about" communications – *i.e.*, communications containing a reference to the name of the tasked account. See [REDACTED]. Based upon the government's descriptions of the proposed collection, the Court understood that the acquisition of Internet communications under Section 702 would be limited to discrete "to/from" communications between or among individual account users and to "about"

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

communications falling within [REDACTED] specific categories that had been first described to the Court in prior proceedings. [REDACTED]

[REDACTED] Declaration of Director of NSA at 20-22. The Court's analysis and ultimate approval of the targeting and minimization procedures in Docket No. [REDACTED], and in the other [REDACTED] Prior 702 Dockets, depended upon the government's representations regarding the scope of the collection. In conducting its review and granting those approvals, the Court did not take into account NSA's acquisition of Internet transactions, which now materially and fundamentally alters the statutory and constitutional analysis.¹⁴

¹⁴ The Court is troubled that the government's revelations regarding NSA's acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program.

In March, 2009, the Court concluded that its authorization of NSA's bulk acquisition of telephone call detail records from [REDACTED] in the so-called "big business records" matter "ha[d] been premised on a flawed depiction of how the NSA uses [the acquired] metadata," and that "[t]his misperception by the FISC existed from the inception of its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government's submissions, and despite a government-devised and Court-mandated oversight regime." Docket No. BR 08-13, March 2, 2009 Order at 10-11. Contrary to the government's repeated assurances, NSA had been routinely running queries of the metadata using querying terms that did not meet the required standard for querying. The Court concluded that this requirement had been "so frequently and systemically violated that it can fairly be said that this critical element of the overall . . . regime has never functioned effectively." *Id.*

Shortly thereafter, the government made a similar disclosure regarding NSA's bulk acquisition of metadata regarding Internet communications in the so-called "big pen register" matter. In [REDACTED] the government reported that, from the time of the initial Court authorization in 2004, NSA had been continually collecting various forms of data falling outside the scope of the Court's orders, and that "[v]irtually every PR/TT record' generated by this program included some data that had not been authorized for collection." Docket No. PR/TT [REDACTED] Mem. Op. at 20-21. This long-running and systemic overcollection had
(continued...)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

The government's submissions make clear not only that NSA has been acquiring Internet transactions since before the Court's approval of the first Section 702 certification in 2008,¹⁵ but also that NSA seeks to continue the collection of Internet transactions. Because NSA's acquisition of Internet transactions presents difficult questions, the Court will conduct its review in two stages. Consistent with the approach it has followed in past reviews of Section 702 certifications and amendments, the Court will first consider the targeting and minimization procedures as applied to the acquisition of communications other than Internet transactions – *i.e.*, to the discrete communications between or among the users of telephone and Internet communications facilities that are to or from a facility tasked for collection.¹⁶ The Court will

¹⁴(...continued)

occurred despite the government's repeated assurances over the course of nearly [REDACTED] years that [REDACTED] authorizations granted by docket number PR/TT [REDACTED] and previous docket numbers only collect, or collected, authorized metadata." *Id.* at 20. The overcollection was not detected by NSA until after an "end-to-end review" of the PR/TT metadata program that had been completed by the agency on August 11, 2009. *Id.*

¹⁵ The government's revelations regarding the scope of NSA's upstream collection implicate 50 U.S.C. § 1809(a), which makes it a crime (1) to "engage[] in electronic surveillance under color of law except as authorized" by statute or (2) to "disclose[] or use[] 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 statute. *See* [REDACTED] (concluding that Section 1809(a)(2) precluded the Court from approving the government's proposed use of, among other things, certain data acquired by NSA without statutory authority through its "upstream collection"). The Court will address Section 1809(a) and related issues in a separate order.

¹⁶ As noted, the Court previously authorized the acquisition of [REDACTED] categories of "about" communications. The Court now understands that all "about" communications are acquired by means of NSA's acquisition of Internet transactions through its upstream collection. *See* June 1 Submission at 1-2, *see also* Sept. 7, 2011 Hearing Tr. at 76. Accordingly, the Court considers the (continued...)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

then assess the effect of the recent disclosures regarding NSA's collection of Internet transactions on its ability to make the findings necessary to approve the certifications and the NSA targeting and minimization procedures.¹⁷

B. The Unmodified Procedures

The government represents that the NSA targeting procedures and the FBI minimization procedures filed with the April 2011 Submissions are identical to the corresponding procedures that were submitted to the Court in Docket Nos. [REDACTED]¹⁸

The Court has reviewed each of these sets of procedures and confirmed that is the case. In fact, the NSA targeting procedures and FBI minimization procedures now before the Court are copies

¹⁶(...continued)

[REDACTED] categories of "about" communications to be a subset of the Internet transactions that NSA acquires. The Court's discussion of the manner in which the government proposes to apply its targeting and minimization procedures to Internet transactions generally also applies to the [REDACTED] categories of "about" communications. See *infra*, pages 41-79.

¹⁷ The FBI and the CIA do not receive unminimized communications that have been acquired through NSA's upstream collection of Internet communications. Sept. 7, 2011 Hearing Tr. at 61-62. Accordingly, the discussion of Internet transactions that appears below does not affect the Court's conclusions that the FBI targeting procedures, the CIA minimization procedures, and the FBI minimization procedures meet the statutory and constitutional requirements.

¹⁸ See Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications for DNI/AG 702(g) Certifications [REDACTED]; Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications for DNI/AG 702(g) Certifications [REDACTED]; Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications for DNI/AG 702(g) Certifications [REDACTED].

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

of the procedures that were initially filed on July 29, 2009, in Docket No. [REDACTED]¹⁹ The Court found in those prior dockets that the targeting and minimization procedures were consistent with the requirements of 50 U.S.C. § 1881a(d)-(e) and with the Fourth Amendment.

See Docket No. [REDACTED]

[REDACTED] The Court is prepared to renew its past findings that the NSA targeting procedures (as applied to forms of to/from communications that have previously been described to the Court) and the FBI minimization procedures are consistent with the requirements of 50 U.S.C. § 1881a(d)-(e) and with the Fourth Amendment.²⁰

C. The Amended Procedures

As noted above, the FBI targeting procedures and the NSA and CIA minimization procedures submitted with the April 2011 Submissions differ in a number of respects from the corresponding procedures that were submitted by the government and approved by the Court in connection with Certifications [REDACTED]. For the reasons that follow, the Court finds that, as applied to the previously authorized collection of discrete communications to or from a tasked facility, the amended FBI targeting procedures and the amended NSA and CIA

¹⁹ Copies of those same procedures were also submitted in Docket Nos. [REDACTED]

²⁰ The Court notes that the FBI minimization procedures are not “set forth in a clear and self-contained manner, without resort to cross-referencing,” as required by FISC Rule 12, which became effective on November 1, 2010. The Court expects that future submissions by the government will comport with this requirement.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

minimization procedures are consistent with the requirements of 50 U.S.C. § 1881a(d)-(e) and with the Fourth Amendment.

1. The Amended FBI Targeting Procedures

The government has made three changes to the FBI targeting procedures, all of which involve Section I.4. That provision requires the FBI, [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

The new language proposed by the government would allow the FBI to [REDACTED]
[REDACTED]

[REDACTED] The government has advised the Court that this change was prompted by the fact that [REDACTED]

[REDACTED] Nevertheless, the current procedures require the FBI to [REDACTED]. The change is intended to eliminate the requirement of [REDACTED].

The second change, reflected in subparagraph (a) of Section I.4, would allow the FBI, under certain circumstances, to [REDACTED]

[REDACTED]

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

[REDACTED]

The above-described changes to the FBI targeting procedures pose no obstacle to a finding by the Court that the FBI targeting procedures are “reasonably designed” to “ensure that any acquisition authorized . . . 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). [REDACTED]

[REDACTED]

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

[REDACTED]

[REDACTED]

Furthermore, as the Court has previously noted, before the FBI targeting procedures are applied, NSA will have followed its own targeting procedures in determining that the user of the facility to be tasked for collection is a non-United States person reasonably believed to be located outside the United States. See Docket No. [REDACTED]. The FBI targeting procedures apply in addition to the NSA targeting procedures, [REDACTED] [REDACTED] Id. The Court has previously found that the NSA targeting procedures proposed for use in connection with Certifications [REDACTED] are reasonably designed to ensure that the users of tasked selectors are non-United States persons reasonably believed to be located outside the United States and also consistent with the Fourth Amendment. See Docket No. [REDACTED] [REDACTED]. It therefore follows that the amended FBI targeting procedures, which provide additional assurance that the users of tasked accounts are non-United States persons located outside the United States, also pass muster.

2. The Amended NSA Minimization Procedures

The most significant change to the NSA minimization procedures regards the rules for querying the data that NSA acquires pursuant to Section 702. The procedures previously approved by the Court effectively impose a wholesale bar on queries using United States-Person identifiers. The government has broadened Section 3(b)(5) to allow NSA to query the vast majority of its Section 702 collection using United States-Person identifiers, subject to approval

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

pursuant to internal NSA procedures and oversight by the Department of Justice.²¹ Like all other NSA queries of the Section 702 collection, queries using United States-person identifiers would be limited to those reasonably likely to yield foreign intelligence information. NSA Minimization Procedures § 3(b)(5). The Department of Justice and the Office of the DNI would be required to conduct oversight regarding NSA's use of United States-person identifiers in such queries. See id.

This relaxation of the querying rules does not alter the Court's prior conclusion that NSA minimization procedures meet the statutory definition of minimization procedures. The Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search Conducted Under the Foreign Intelligence Surveillance Act ("FBI SMPs") contain an analogous provision allowing queries of unminimized FISA-acquired information using identifiers – including United States-person identifiers – when such queries are designed to yield foreign intelligence information. See FBI SMPs § III.D. In granting hundreds of applications for electronic surveillance or physical search since 2008, including applications targeting United States persons and persons in the United States, the Court has found that the FBI SMPs meet the definitions of minimization procedures at 50 U.S.C. §§ 1801(h) and 1821(4). It follows that the substantially-similar

²¹ The government is still in the process of developing its internal procedures and will not permit NSA analysts to begin using United States-person identifiers as selection terms until those procedures are completed. June 28 Submission at 4 n.3. In addition, the government has clarified that United States-person identifiers will not be used to query the fruits of NSA's upstream collection. Aug. 30 Submission at 11. NSA's upstream collection acquires approximately 9% of the total Internet communications acquired by NSA under Section 702. Aug. 16 Submission at 2.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

querying provision found at Section 3(b)(5) of the amended NSA minimization procedures should not be problematic in a collection that is focused on non-United States persons located outside the United States and that, in the aggregate, is less likely to result in the acquisition of nonpublic information regarding non-consenting United States persons.

A second change to the NSA minimization procedures is the addition of language specifying that the five-year retention period for communications that are not subject to earlier destruction runs from the expiration date of the certification authorizing the collection. See NSA Minimization Procedures, §§ 3(b)(1), 3(c), 5(3)(b), and 6(a)(1)(b). The NSA minimization procedures that were previously approved by the Court included a retention period of five years, but those procedures do not specify when the five-year period begins to run. The change proposed here harmonizes the procedures with the corresponding provision of the FBI minimization procedures for Section 702 that has already been approved by the Court. See FBI Minimization Procedures at 3 (¶ j).

The two remaining changes to the NSA minimization procedures are intended to clarify the scope of the existing procedures. The government has added language to Section 1 to make explicit that the procedures apply not only to NSA employees, but also to any other persons engaged in Section 702-related activities that are conducted under the direction, authority or control of the Director of NSA. NSA Minimization Procedures at 1. According to the government, this new language is intended to clarify that Central Security Service personnel conducting signals intelligence operations authorized by Section 702 are bound by the procedures, even when they are deployed with a military unit and subject to the military chain of

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

command. The second clarifying amendment is a change to the definition of “identification of a United States person” in Section 2. The new language eliminates a potential ambiguity that might have resulted in the inappropriate treatment of the name, unique title, or address of a United States person as non-identifying information in certain circumstances. *Id.* at 2. These amendments, which resolve any arguable ambiguity in favor of broader application of the protections found in the procedures, raise no concerns.

3. The Amended CIA Minimization Procedures

The CIA minimization procedures include a new querying provision similar to the provision that the government proposes to add to the NSA minimization procedures and that is discussed above. CIA Minimization Procedures § 4. The new language would allow the CIA to conduct queries of Section 702-acquired information using United States-person identifiers. All CIA queries of the Section 702 collection would be subject to review by the Department of Justice and the Office of the DNI. *See id.* For the reasons stated above with respect to the relaxed querying provision in the amended NSA minimization procedures, the addition of the new CIA querying provision does not preclude the Court from concluding that the amended CIA minimization procedures satisfy the statutory definition of minimization procedures and comply with the Fourth Amendment.²²

The amended CIA minimization procedures include a definition of “United States person identity,” a term that is not defined in the current version of the procedures. CIA Minimization

²² The Court understands that NSA does not share its upstream collection in unminimized form with the CIA. [REDACTED]

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Procedures § 1.b. The proposed definition closely tracks the revised definition of “identification of a United States person” that is included in the amended NSA minimization procedures and discussed above. For the same reasons, the addition of this definition, which clarifies the range of protected information, raises no concerns in the context of the CIA minimization procedures.

Another new provision of the CIA minimization procedures prescribes the manner in which the CIA must store unminimized Section 702-acquired communications. See CIA Minimization Procedures § 2. The same provision establishes a default retention period for unminimized communications that do not qualify for longer retention under one of three separate provisions. See id. Absent an extension by the Director of the National Clandestine Service or one of his superiors, that default retention period is five years from the date of the expiration of the certification authorizing the collection. Id. As noted above, this is the same default retention period that appears in the FBI minimization procedures that have previously been approved by the Court. See FBI Minimization Procedures at 3 (¶ j).

The government also has added new language to the CIA minimization procedures to clarify that United States person information deemed to qualify for retention based on its public availability or on the consent of the person to whom it pertains may be kept indefinitely and stored separately from the unminimized information subject to the default storage and retention rules set forth in new Section 2, which is discussed above. CIA Minimization Procedures § 2. Because FISA’s minimization requirements are limited to the acquisition, retention, and dissemination of “nonpublicly available information concerning unconsenting United States persons,” this provision raises no statutory concern. See 50 U.S.C. §§ 1801(h)(1), 1821(4)(A)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

(emphasis added). It likewise raises no Fourth Amendment problem. See Katz v. United States, 389 U.S. 347, 351 (1967) (“What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.”).

Finally, a new provision would expressly allow the CIA to retain information acquired pursuant to Section 702 in emergency backup systems that may be used to restore data in the event of a system failure. CIA Minimization Procedures § 6(e). Only non-analyst technical personnel will have access to data stored in data backup systems. Id. Further, in the event that such systems are used to restore lost, destroyed, or inaccessible data, the CIA must apply its minimization procedures to the transferred data. Id. The FBI minimization procedures that have previously been approved by the Court contemplate the storage of Section 702 collection in emergency backup systems that are not accessible to analysts, subject to similar restrictions. See FBI Minimization Procedures at 2 (¶ e.3). The Court likewise sees no problem with the addition of Section 6(e) to the CIA minimization procedures.

D. The Effect of the Government’s Disclosures Regarding NSA’s Acquisition of Internet Transactions

Based on the government’s prior representations, the Court has previously analyzed NSA’s targeting and minimization procedures only in the context of NSA acquiring discrete communications. Now, however, in light of the government’s revelations as to the manner in which NSA acquires Internet communications, it is clear that NSA acquires “Internet

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Fourth Amendment.

For the reasons set forth below, the Court finds that NSA's targeting procedures, as the government proposes to implement them in connection with MCTs, are consistent with the requirements of 50 U.S.C. §1881a(d)(1). However, the Court is unable to find that NSA's minimization procedures, as the government proposes to apply them in connection with MCTs, are "reasonably designed in light of the purpose and technique of the particular [surveillance or physical search], 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." 50 U.S.C. §§ 1801(h)(1) & 1821(4)(A). The Court is also unable to find that NSA's targeting and minimization procedures, as the government proposes to implement them in connection with MCTs, are consistent with the Fourth Amendment.

1. The Scope of NSA's Upstream Collection

NSA acquires more than two hundred fifty million Internet communications each year pursuant to Section 702, but the vast majority of these communications are obtained from Internet service providers and are not at issue here.²⁴ Sept. 9 Submission at 1; Aug. 16 Submission at Appendix A. Indeed, NSA's upstream collection constitutes only approximately

²⁴ In addition to its upstream collection, NSA acquires discrete Internet communications from Internet service providers such as [REDACTED] [REDACTED] [REDACTED] Aug. 16 Submission at 2; Aug. 30 Submission at 11; see also Sept. 7, 2011 Hearing Tr. at 75-77. NSA refers to this non-upstream collection as its "PRISM collection." Aug. 30 Submission at 11. The Court understands that NSA does not acquire "Internet transactions" through its PRISM collection. See Aug. 16 Submission at 1.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

9% of the total Internet communications being acquired by NSA under Section 702. Sept. 9 Submission at 1; Aug. 16 Submission at 2.

Although small in relative terms, NSA's upstream collection is significant for three reasons. First, NSA's upstream collection is "uniquely capable of acquiring certain types of targeted communications containing valuable foreign intelligence information."²⁵ Docket No. [REDACTED].

Second, the Court now understands that, in order to collect those targeted Internet communications, NSA's upstream collection devices acquire Internet transactions, and NSA acquires millions of such transactions each year.²⁶ Third, the government has acknowledged that, due to the technological challenges associated with acquiring Internet transactions, NSA is unable to exclude certain Internet transactions from its upstream collection. See June 1 Submission at 3-12.

In its June 1 Submission, the government explained that NSA's upstream collection devices have technological limitations that significantly affect the scope of collection. [REDACTED]

[REDACTED]

²⁵ [REDACTED]

²⁶ NSA acquired more than 13.25 million Internet transactions through its upstream collection between January 1, 2011, and June 30, 2011. See Aug. 16 Submission at 2; see also Sept. 9 Submission at 1-2.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

[REDACTED]. See id. at 7. Moreover, at the time of acquisition, 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 may be to, from, or about a tasked selector.²⁷ Id. at 2.

As a practical matter, this means that NSA's upstream collection devices acquire any Internet transaction transiting the device if the transaction contains a targeted selector anywhere within it, and:

[REDACTED]

See id. at 6.

The practical implications of NSA's acquisition of Internet transactions through its upstream collection for the Court's statutory and Fourth Amendment analyses are difficult to assess. The sheer volume of transactions acquired by NSA through its upstream collection is such that any meaningful review of the entire body of the transactions is not feasible. As a result, the Court cannot know for certain the exact number of wholly domestic communications acquired through this collection, nor can it know the number of non-target communications

[REDACTED]

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

acquired or the extent to which those communications are to or from United States persons or persons in the United States. Instead, NSA and the Court can only look at samples of the data and then draw whatever reasonable conclusions they can from those samples. Even if the Court accepts the validity of conclusions derived from statistical analyses, there are significant hurdles in assessing NSA's upstream collection. Internet service providers are constantly changing their protocols and the services they provide, and often give users the ability to customize how they use a particular service.²⁸ *Id.* at 24-25. As a result, it is impossible to define with any specificity the universe of transactions that will be acquired by NSA's upstream collection at any point in the future.

Recognizing that further revelations concerning what NSA has actually acquired through its 702 collection, together with the constant evolution of the Internet, may alter the Court's analysis at some point in the future, the Court must, nevertheless, consider whether NSA's targeting and minimization procedures are consistent with FISA and the Fourth Amendment based on the record now before it. In view of the revelations about how NSA is actually conducting its upstream collection, two fundamental underpinnings of the Court's prior assessments no longer hold true.

28



~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

First, the Court previously understood that NSA's technical measures²⁹ would prevent the acquisition of any communication as to which the sender and all intended recipients were located in the United States ("wholly domestic communication") except for "theoretically possible" cases

[REDACTED]

[REDACTED]

[REDACTED] The Court now understands, however, that NSA has acquired, is acquiring, and, if the certifications and procedures now before the Court are approved, will continue to acquire, tens of thousands of wholly domestic communications. NSA's manual review of a statistically representative sample drawn from its upstream collection³⁰ reveals that NSA acquires approximately 2,000-10,000 MCTs each year that contain at least one wholly domestic communication.³¹ See Aug. 16 Submission at 9. In addition to these MCTs, NSA

²⁹ [REDACTED]

³⁰ In an effort to address the Court's concerns, NSA conducted a manual review of a random sample consisting of 50,440 Internet transactions taken from the more than 13.25 million Internet transactions acquired through NSA's upstream collection during a six month period. See generally Aug. 16 Submission (describing NSA's manual review and the conclusions NSA drew therefrom). The statistical conclusions reflected in this Memorandum Opinion are drawn from NSA's analysis of that random sample.

³¹ Of the approximately 13.25 million Internet transactions acquired by NSA through its upstream collection during the six-month period, between 996 and 4,965 are MCTs that contain a wholly domestic communication not to, from, or about a tasked selector. Aug. 16 Submission at 9.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

likely acquires tens of thousands more wholly domestic communications every year,³² given that NSA's upstream collection devices will acquire a wholly domestic "about" SCT if it is routed internationally.³³ Moreover, the actual number of wholly domestic communications acquired

³² NSA's manual review focused on examining the MCTs acquired through NSA's upstream collection in order to assess whether any contained wholly domestic communications. Sept. 7, 2011 Hearing Tr. at 13-14. As a result, once NSA determined that a transaction contained a single, discrete communication, no further analysis of that transaction was done. See Aug. 16 Submission at 3. After the Court expressed concern that this category of transactions might also contain wholly domestic communications, NSA conducted a further review. See Sept. 9 Submission at 4. NSA ultimately did not provide the Court with an estimate of the number of wholly domestic "about" SCTs that may be acquired through its upstream collection. Instead, NSA has concluded that "the probability of encountering wholly domestic communications in transactions that feature only a single, discrete communication should be smaller – and certainly no greater – than potentially encountering wholly domestic communications within MCTs." Sept. 13 Submission at 2.

The Court understands this to mean that the percentage of wholly domestic communications within the universe of SCTs acquired through NSA's upstream collection should not exceed the percentage of MCTs containing a wholly domestic communication that NSA found when it examined all of the MCTs within its statistical sample. Since NSA found 10 MCTs with wholly domestic communications within the 5,081 MCTs reviewed, the relevant percentage is .197% (10/5,081). Aug. 16 Submission at 5.

NSA's manual review found that approximately 90% of the 50,440 transactions in the sample were SCTs. Id. at 3. Ninety percent of the approximately 13.25 million total Internet transactions acquired by NSA through its upstream collection during the six-month period, works out to be approximately 11,925,000 transactions. Those 11,925,000 transactions would constitute the universe of SCTs acquired during the six-month period, and .197% of that universe would be approximately 23,000 wholly domestic SCTs. Thus, NSA may be acquiring as many as 46,000 wholly domestic "about" SCTs each year, in addition to the 2,000-10,000 MCTs referenced above.

³³ 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 (b) (1) [REDACTED] will at the very least travel from the (b) (1) [REDACTED] user's own computer, to (b) (1) (A) [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 any particular leg of the route need only identify the IP

(continued...)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

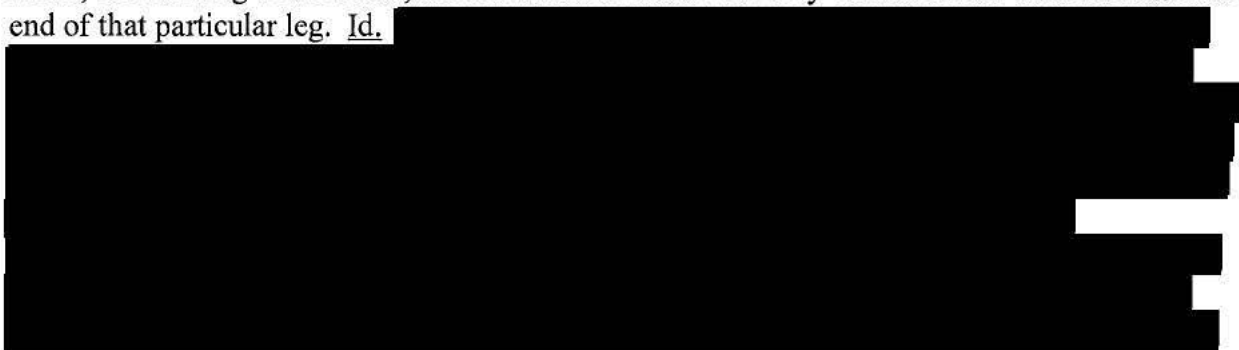
~~TOP SECRET//COMINT//ORCON,NOFORN~~

may be still higher in view of NSA's inability conclusively to determine whether a significant portion of the MCTs within its sample contained wholly domestic communications.³⁴

Second, the Court previously understood that NSA's upstream collection would only acquire the communication of a United States person or a person in the United States if: 1) that

³³(...continued)

addresses 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.*



³⁴ During its manual review, NSA was unable to determine whether 224 of the 5,081 MCTs reviewed contained any wholly domestic communications, because the transactions lacked sufficient information for NSA to determine the location or identity of the "active user" (*i.e.*, the individual using the electronic communications account/address/identifier to interact with his/her Internet service provider). Aug. 16 Submission at 7. NSA then conducted an intensive review of all available information for each of these MCTs, including examining the contents of each discrete communication contained within it, but was still unable to determine conclusively whether any of these MCTs contained wholly domestic communications. Sept. 9 Submission at 3. NSA asserts that "it is reasonable to presume that [the] 224 MCTs do not contain wholly domestic communications," but concedes that, due to the limitations of the technical means used to prevent the acquisition of wholly domestic communications, NSA may acquire wholly domestic communications. *See* Aug. 30 Submission at 7-8. The Court is prepared to accept that the number of wholly domestic communications acquired in this category of MCTs is relatively small, for the reasons stated in the government's August 30 Submission. However, when considering NSA's upstream collection as a whole, and the limitations of NSA's technical means, the Court is not prepared to presume that the number of wholly domestic communications contained within this category of communications will be zero. Accordingly, the Court concludes that this category of communications acquired through NSA's upstream collection may drive the total number of wholly domestic communications acquired slightly higher.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

person was in direct contact with a targeted selector; 2) the communication referenced the targeted selector, and the communication fell into one of [REDACTED] specific categories of “about” communications; or 3) despite the operation of the targeting procedures, United States persons or persons inside the United States were mistakenly targeted. See Docket No. [REDACTED]

[REDACTED]. But the Court now understands that, in addition to these communications, NSA’s upstream collection also acquires: a) the communications of United States persons and persons in the United States that are not to, from, or about a tasked selector and that are acquired solely because the communication is contained within an MCT that somewhere references a tasked selector [REDACTED] [REDACTED] and b) any Internet transaction that references a targeted selector, regardless of whether the transaction falls within one of the [REDACTED] previously identified categories of “about communications,” see June 1 Submission at 24-27. [REDACTED]

On the current record, it is difficult to assess how many MCTs acquired by NSA actually contain a communication of or concerning a United States person,³⁵ or a communication to or from a person in the United States. This is because NSA’s manual review of its upstream collection focused primarily on wholly domestic communications – *i.e.*, if one party to the

³⁵ NSA’s minimization procedures define “[c]ommunications of a United States person” to include “all communications to which a United States person is a party.” NSA Minimization Procedures § 2(c). “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. *Id.* § 2(b).

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

communication was determined to be outside the United States, the communication was not further analyzed. Aug. 16 Submission at 1-2. Nevertheless, NSA's manual review did consider the location and identity of the active user for each MCT acquired, and this information – when considered together with certain presumptions – shows that NSA is likely acquiring tens of thousands of discrete communications of non-target United States persons and persons in the United States, by virtue of the fact that their communications are included in MCTs selected for acquisition by NSA's upstream collection devices.³⁶

To illustrate, based upon NSA's analysis of the location and identity of the active user for the MCTs it reviewed, MCTs can be divided into four categories:

1. MCTs as to which the active user is the user of the tasked facility (i.e., the target of the acquisition) and is reasonably believed to be located outside the United States;³⁷
2. MCTs as to which the active user is a non-target who is believed to be located inside the United States;
3. MCTs as to which the active user is a non-target who is believed to be located outside the United States; and

³⁶ Although there is some overlap between this category of communications and the tens of thousands of wholly domestic communications discussed above, the overlap is limited to MCTs containing wholly domestic communications. To the extent that the wholly domestic communications acquired are SCTs, they are excluded from the MCTs referenced here. Similarly, to the extent communications of non-target United States persons and persons in the United States that are contained within the tens of thousands of MCTs referenced here are not wholly domestic, they would not be included in the wholly domestic communications referenced above.

³⁷ Although it is possible for an active user target to be located in the United States, NSA's targeting procedures require NSA to terminate collection if it determines that a target has entered the United States. NSA Targeting Procedures at 7-8. Accordingly, the Court excludes this potential category from its analysis.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

4. MCTs as to which the active user's identity or location cannot be determined.

Aug. 16 Submission at 4-8.

With regard to the first category, if the target is the active user, then it is reasonable to presume that all of the discrete communications within an MCT will be to or from the target. Although United States persons and persons in the United States may be party to any of those communications, NSA's acquisition of such communications is of less concern than the communications described in the following categories because the communicants were in direct communication with a tasked facility, and the acquisition presumptively serves the foreign intelligence purpose of the collection. NSA acquires roughly 300-400 thousand such MCTs per year.³⁸

For the second category, since the active user is a non-target who is located inside the United States, there is no reason to believe that all of the discrete communications contained within the MCTs will be to, from, or about the targeted selector (although there would need to be at least one such communication in order for NSA's upstream devices to acquire the transaction). Further, because the active user is in the United States, the Court presumes that the majority of that person's communications will be with other persons in the United States, many of whom will be United States persons. NSA acquires approximately 7,000-8,000 such MCTs per year, each of which likely contains one or more non-target discrete communications to or from other

³⁸ NSA acquired between 168,853 and 206,922 MCTs as to which the active user was the target over the six-month period covered by the sample. Aug. 16 Submission at 9.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

persons in the United States.³⁹

The third category is similar to the second in that the active user is a non-target. Therefore, there is no reason to believe that all of the communications within the MCTs will be to, from, or about the targeted selector (although there would need to be at least one such communication in order for NSA's upstream devices to acquire the transaction). However, because the active user is believed to be located outside the United States, the Court presumes that most of that persons's communications will be with other persons who are outside the United States, most of whom will be non-United States persons. That said, the Court notes that some of these MCTs are likely to contain non-target communications of or concerning United States persons, or that are to or from a person in the United States.⁴⁰ The Court has no way of knowing precisely how many such communications are acquired. Nevertheless, it appears that NSA acquires at least 1.3 million such MCTs each year,⁴¹ so even if only 1% of these MCTs

³⁹ In its manual review, NSA identified ten MCTs as to which the active user was in the United States and that contained at least one wholly domestic communication. See Aug. 16 Submission at 5-7. NSA also identified seven additional MCTs as to which the active user was in the United States. Id. at 5. Although NSA determined that at least one party to each of the communications within the seven MCTs was reasonably believed to be located outside the United States, NSA did not indicate whether any of the communicants were United States persons or persons in the United States. Id. The Court sees no reason to treat these two categories of MCTs differently because the active users for both were in the United States. Seventeen MCTs constitutes .3% of the MCTs reviewed (5,081), and .3% of the 1.29-1.39 million MCTs NSA acquires every six months (see id. at 8) is 3,870- 4,170, or 7,740-8,340 every year.

⁴⁰ The government has acknowledged as much in its submissions. See June 28 Submission at 5.

⁴¹ Based on its manual review, NSA assessed that 2668 of the 5,081 MCTs reviewed
(continued...)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

contain a single non-target communication of or concerning a United States person, or that is to or from a person in the United States, NSA would be acquiring in excess of 10,000 additional discrete communications each year that are of or concerning United States persons, or that are to or from a person in the United States.

The fourth category is the most problematic, because without the identity of the active user – i.e., whether the user is the target or a non-target – or the active user's location, it is difficult to determine what presumptions to make about these MCTs. NSA acquires approximately 97,000-140,000 such MCTs each year.⁴² In the context of wholly domestic communications, the government urges the Court to apply a series of presumptions that lead to the conclusion that this category would not contain any wholly domestic communications. Aug. 30 Submission at 4-8. The Court questions the validity of those presumptions, as applied to wholly domestic communications, but certainly is not inclined to apply them to assessing the likelihood that MCTs might contain communications of or concerning United States persons, or communications to or from persons in the United States. The active users for some of these

⁴¹(...continued)

(approximately 52%) had a non-target active user who was reasonably believed to be located outside the United States. Aug. 16 Submission at 4-5. Fifty-two percent of the 1.29 to 1.39 million MCTs that NSA assessed were acquired through its upstream collection every six months would work out to 670,800 - 722,800 MCTs, or approximately 1.3-1.4 million MCTs per year that have a non-target active user believed to be located outside the United States.

⁴² NSA determined that 224 MCTs of the 5,081 MCTs acquired during a six-month period (b) (1) (A)

From this, NSA concluded that it acquired between 48,609 and 70,168 such MCTs every six months through its upstream collection (or approximately 97,000-140,000 such MCTs each year). Id. at 9 n.27.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

MCTs may be located in the United States, and, even if the active user is located overseas, the MCTs may contain non-target communications of or concerning United States persons or that are to or from persons in the United States. Accordingly, this “unknown” category likely adds substantially to the number of non-target communications of or concerning United States persons or that are to or from persons in the United States being acquired by NSA each year.

In sum, then, NSA’s upstream collection is a small, but unique part of the government’s overall collection under Section 702 of the FAA. NSA acquires valuable information through its upstream collection, but not without substantial intrusions on Fourth Amendment-protected interests. Indeed, the record before this Court establishes that NSA’s acquisition of Internet transactions likely results in NSA acquiring annually tens of thousands of wholly domestic communications, and tens of thousands of non-target communications of persons who have little or no relationship to the target but who are protected under the Fourth Amendment. Both acquisitions raise questions as to whether NSA’s targeting and minimization procedures comport with FISA and the Fourth Amendment.

2. NSA’s Targeting Procedures

The Court will first consider whether NSA’s acquisition of Internet transactions through its upstream collection, as described above, means that NSA’s targeting procedures, as implemented, are not “reasonably designed” to: 1) “ensure that any acquisition authorized under [the certifications] is limited to targeting persons reasonably believed to be located outside the United States”; and 2) “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

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

that references the tasked selector, but also in many cases the contents of other discrete communications that do not reference the tasked selector and to which no target is a party. See May 2 Letter at 2-3 [REDACTED] By acquiring such MCTs, NSA likely acquires tens of thousands of additional communications of non-targets each year, many of whom have no relationship whatsoever with the user of the tasked selector. While the Court has concerns about NSA's acquisition of these non-target communications, the Court accepts the government's representation that the "sole reason [a non-target's MCT] is selected for acquisition is that it contains the presence of a tasked selector used by a person who has been subjected to NSA's targeting procedures." June 1 Submission at 4. Moreover, at the time of acquisition, NSA's upstream collection devices often lack the capability to determine whether a transaction contains a single communication or multiple communications, or to identify the parties to any particular communication within a transaction. See id. Therefore, the Court has no reason to believe that NSA, by acquiring Internet transactions containing multiple communications, is targeting anyone other than the user of the tasked selector. See United States v. Chemical Found., Inc., 272 U.S. 1, 14-15 (1926) ("The presumption of regularity supports the official acts of public officers, and, in the absence of clear evidence to the contrary, courts presume that they have properly discharged their official duties.").

b. Acquisition of Wholly Domestic Communications

NSA's acquisition of Internet transactions complicates the analysis required by Section 1881a(d)(1)(B), since the record shows that the government knowingly acquires tens of thousands of wholly domestic communications each year. At first blush, it might seem obvious

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

that targeting procedures that permit such acquisitions could not be “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 in the United States.” 50 U.S.C. § 1881a(d)(1)(B). However, a closer examination of the language of the statute leads the Court to a different conclusion.

The government focuses primarily on the “intentional acquisition” language in Section 1881a(d)(1)(B). Specifically, the government argues that NSA is not “intentionally” acquiring wholly domestic communications because the government does not intend to acquire transactions containing communications that are wholly domestic and has implemented technical means to prevent the acquisition of such transactions. See June 28 Submission at 12. This argument fails for several reasons.

NSA targets a person under Section 702 certifications by acquiring communications to, from, or about a selector used by that person. Therefore, to the extent NSA’s upstream collection devices acquire an Internet transaction containing a single, discrete communication that is to, from, or about a tasked selector, it can hardly be said that NSA’s acquisition is “unintentional.” In fact, the government has argued, and the Court has accepted, that the government intentionally acquires communications to and from a target, even when NSA reasonably – albeit mistakenly – believes that the target is located outside the United States. See Docket No. [REDACTED]
[REDACTED]

With respect to MCTs, the sole reason NSA acquires such transactions is the presence of a tasked selector within the transaction. Because it is technologically infeasible for NSA’s

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

upstream collection devices to acquire only the discrete communication to, from, or about a tasked selector that may be contained within an MCT, however, the government argues that the only way to obtain the foreign intelligence information found within the discrete communication is to acquire the entire transaction in which it is contained. June 1 Submission at 21. As a result, the government intentionally acquires all discrete communications within an MCT, including those that are not to, from or about a tasked selector. See June 28 Submission at 12, 14; see also Sept. 7, 2011 Hearing Tr. at 33-34.

The fact that NSA's technical measures cannot prevent NSA from acquiring transactions containing wholly domestic communications under certain circumstances does not render NSA's acquisition of those transactions "unintentional." The government repeatedly characterizes such acquisitions as a "failure" of NSA's "technical means." June 28 Submission at 12; see also Sept. 7, 2011 Hearing Tr. at 35-36. However, there is nothing in the record to suggest that NSA's technical means are malfunctioning or otherwise failing to operate as designed. 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. See June 1 Submission at 29. And in the case of MCTs containing wholly domestic communications that are not to, from, or about a tasked selector, NSA has no way to determine, at the time of acquisition, that a particular communication within an MCT is wholly domestic. See id. Furthermore, now that NSA's manual review of a sample of its upstream collection has confirmed that NSA likely acquires tens of thousands of wholly domestic communications each year, there is no question that the

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

government is knowingly acquiring Internet transactions that contain wholly domestic communications through its upstream collection.⁴³

The government argues that an NSA analyst's post-acquisition discovery that a particular Internet transaction contains a wholly domestic communication should retroactively render NSA's acquisition of that transaction "unintentional." June 28 Submission at 12. That argument is unavailing. NSA's collection devices are set to acquire transactions that contain a reference to the targeted selector. When the collection device acquires such a transaction, it is functioning precisely as it is intended, even when the transaction includes a wholly domestic communication. The language of the statute makes clear that it is the government's intention at the time of acquisition that matters, and the government conceded as much at the hearing in this matter. Sept. 7, 2011 Hearing Tr. at 37-38.

Accordingly, the Court finds that NSA intentionally acquires Internet transactions that reference a tasked selector through its upstream collection with the knowledge that there are tens of thousands of wholly domestic communications contained within those transactions. But this is not the end of the analysis. To return to the language of the statute, NSA's targeting procedures must be 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

⁴³ It is generally settled that a person intends to produce a consequence either (a) when he acts with a purpose of producing that consequence or (b) when he acts knowing that the consequence is substantially certain to occur. Restatement (Third) of Torts § 1 (2010); see also United States v. Dyer, 589 F.3d 520, 528 (1st Cir. 2009) (in criminal law, "'intent' ordinarily requires only that the defendant reasonably knew the proscribed result would occur"), cert. denied, 130 S. Ct. 2422 (2010).

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

acquisition to be located in the United States.” 50 U.S.C. § 1881a(d)(1)(B) (emphasis added).

The underscored language requires an acquisition-by-acquisition inquiry. Thus, the Court must consider whether, at the time NSA intentionally acquires a transaction through its upstream collection, NSA will know that the sender and all intended recipients of any particular communication within that transaction are located in the United States.

Presently, it is not technically possible for NSA to configure its upstream collection devices (b) (1) (A)

[REDACTED]

[REDACTED] the practical effect of this technological limitation is that NSA cannot know at the time it acquires an Internet transaction whether the sender and all intended recipients of any particular discrete communication contained within the transaction are located inside the United States.

[REDACTED]

⁴⁴ See supra, note 33.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Given that NSA's upstream collection devices lack the capacity to detect wholly domestic communications at the time an Internet transaction is acquired, the Court is inexorably led to the conclusion 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 in the United States. This is true despite the fact that NSA knows with certainty that the upstream collection, viewed as a whole, results in the acquisition of wholly domestic communications.

By expanding its Section 702 acquisitions to include the acquisition of Internet transactions through its upstream collection, NSA has, as a practical matter, circumvented the spirit of Section 1881a(b)(4) and (d)(1) with regard to that collection. NSA's knowing acquisition of tens of thousands of wholly domestic communications through its upstream collection is a cause of concern for the Court. But the meaning of the relevant statutory provision is clear and application to the facts before the Court does not lead to an impossible or absurd result. The Court's review does not end with the targeting procedures, however. The Court must

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

also consider whether NSA's minimization procedures are consistent with §1881a(e)(1) and whether NSA's targeting and minimization procedures are consistent with the requirements of the Fourth Amendment.

3. NSA's Minimization Procedures, As Applied to MCTs in the Manner Proposed by the Government, Do Not Meet FISA's Definition of "Minimization Procedures"

The Court next considers whether NSA's minimization procedures, as the government proposes to apply them to Internet transactions, meet the statutory requirements. As noted above, 50 U.S.C. § 1881a(e)(1) requires that the minimization procedures "meet the definition of minimization procedures under [50 U.S.C. §§] 1801(h) or 1821(4)" That definition requires "specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular [surveillance or physical search], 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." 50 U.S.C. §§ 1801(h)(1) & 1821(4)(A). For the reasons stated below, the Court concludes that NSA's minimization procedures, as applied to MCTs in the manner proposed by the government, do not meet the statutory definition in all respects.

a. The Minimization Framework

NSA's minimization procedures do not expressly contemplate the acquisition of MCTs, and the language of the procedures does not lend itself to straightforward application to MCTs. Most notably, various provisions of the NSA minimization procedures employ the term

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

“communication” as an operative term. As explained below, for instance, the rules governing retention, handling, and dissemination vary depending whether or not a communication is deemed to constitute a “domestic communication” instead of a “foreign communication,” see NSA Minimization Procedures §§ 2(e), 5, 6, 7; a communication “of” or “concerning” a U.S. person, see id. §§ 2(b)-(c), 3(b)(1)-(2), 3(c); a “communication to, from, or about a target,” id. § 3(b)(4); or a “communication . . . reasonably believed to contain foreign intelligence information or evidence of a crime,” id. But MCTs can be fairly described as communications that contain several smaller communications. Applying the terms of the NSA minimization procedures to MCTs rather than discrete communications can produce very different results.

In a recent submission, the government explained how NSA proposes to apply its minimization procedures to MCTs. See Aug. 30 Submission at 8-11.⁴⁵ Before discussing the measures proposed by the government for handling MCTs, it is helpful to begin with a brief overview of the NSA minimization procedures themselves. The procedures require that all acquisitions “will be conducted in a manner designed, to the greatest extent feasible, to minimize the acquisition of information not relevant to the authorized purpose of the collection.” NSA

⁴⁵ Although NSA has been collecting MCTs since before the Court’s approval of the first Section 702 certification in 2008, see June 1 Submission at 2, it has not, to date, applied the measures proposed here to the fruits of its upstream collection. Indeed, until NSA’s manual review of a six-month sample of its upstream collection revealed the acquisition of wholly domestic communications, the government asserted that NSA had never found a wholly domestic communication in its upstream collection. See id.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Minimization Procedures § 3(a).⁴⁶ Following acquisition, the procedures require that, “[a]s 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.” *Id.* § 3(b)(4). “Foreign communication means a communication that has at least one communicant outside of the United States.” *Id.* § 2(e). “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.” *Id.* In addition, domestic communications include “[a]ny 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 the targeting was believed to be a non-United States person but was in fact a United States person” *Id.* § 3(d)(2). A domestic communication must be “promptly destroyed upon recognition unless the Director (or Acting Director) of NSA specifically determines, in writing, that” the communication contains foreign intelligence

⁴⁶ Of course, NSA’s separate targeting procedures, discussed above, also govern the manner in which communications are acquired.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

information or evidence of a crime, or that it falls into another narrow exception permitting retention. See id. § 5.⁴⁷

Upon determining that a communication is a “foreign communication,” NSA must decide whether the communication is “of” or “concerning” a United States person. Id. § 6.

“Communications of a United States person include all communications to which a United States person is a party.” Id. § 2(c). “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.” Id. § 2(b).

A foreign communication that is of or concerning a United States person and that is determined to contain neither foreign intelligence information nor evidence of a crime must be destroyed “at the earliest practicable point in the processing cycle,” and “may be retained no longer than five years from the expiration date of the certification in any event.” Id. § 3(b)(1).⁴⁸

⁴⁷ Once such a determination is made by the Director, the domestic communications at issue are effectively treated as “foreign communications” for purposes of the rules regarding retention and dissemination.

⁴⁸ Although Section 3(b)(1) by its terms applies only to “inadvertently acquired communications of or concerning a United States person,” the government has informed the Court that this provision is intended to apply, and in practice is applied, to all foreign communications of or concerning United States persons that contain neither foreign intelligence information nor evidence of a crime. Docket No. 702(i)-08-01, Sept. 2, 2008 Notice of Clarification and Correction at 3-5. Moreover, Section 3(c) of the procedures separately provides that foreign communications that do not qualify for retention and that “are known to contain communications of or concerning United States persons will be destroyed upon recognition,” and, like unreviewed communications, “may be retained no longer than five years from the

(continued...)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

A foreign communication that is of or concerning a United States person may be retained indefinitely if the “dissemination of such communications with reference to such United States persons would be permitted” under the dissemination provisions that are discussed below, or if it contains evidence of a crime. Id. § 6(a)(2)-(3). If the retention of a foreign communication of or concerning a United States person is “necessary for the maintenance of technical databases,” it may be retained for five years to allow for technical exploitation, or for longer than five years if more time is required for decryption or if the NSA Signals Intelligence Director “determines in writing that retention for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements.” Id. § 6(a)(1).

As a general rule, “[a] report based on communications of or concerning a United States person may be disseminated” only “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.” Id. § 6(b). A report including the identity of the United States person may be provided to a “recipient requiring the identity of such person for the performance of official duties,” but only if at least one of eight requirements is also met – for instance, if “the identity of the United States person is necessary to understand foreign intelligence information or assess its importance,” or if “information indicates the United States

⁴⁸(...continued)
expiration date of the certification authorizing the collection in any event.”

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

person may be . . . an agent of a foreign power” or that he is “engaging in international terrorism activities.” Id.⁴⁹

b. Proposed Minimization Measures for MCTs

The government proposes that NSA’s minimization procedures be applied to MCTs in the following manner. After acquisition, upstream acquisitions, including MCTs, will reside in NSA repositories until they are accessed (e.g., in response to a query) by an NSA analyst performing his or her day-to-day work. NSA proposes adding a “cautionary banner” to the tools its analysts use to view the content of communications acquired through upstream collection under Section 702. See Aug. 30 Submission at 9. The banner, which will be “broadly displayed on [such] tools,” will “direct analysts to consult guidance on how to identify MCTs and how to handle them.” Id. at 9 & n.6.⁵⁰ Analysts will be trained to identify MCTs and to recognize wholly domestic communications contained within MCTs. See id. at 8-9.

When an analyst identifies an upstream acquisition as an MCT, the analyst will decide whether or not he or she “seek[s] to use a discrete communication within [the] MCT,”

⁴⁹ The procedures also permit NSA to provide unminimized communications to the CIA and FBI (subject to their own minimization procedures), and to foreign governments for the limited purpose of obtaining “technical and linguistic assistance.” NSA Minimization Procedures §§ 6(c), 8(b). Neither of these provisions has been used to share upstream acquisitions. Sept. 7, 2011 Hearing Tr. at 61-62.

⁵⁰ The banner will not be displayed for communications that “can be first identified through technical means where the active user is NSA’s tasked selector or that contain only a single, discrete communication based on particular stable and well-known protocols.” Aug. 30 Submission at 9 n.6. See infra, note 27, and supra, note 54.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

presumably by reviewing some or all of the MCT's contents. Id. at 8.⁵¹ "NSA analysts seeking to use a discrete communication contained in an MCT (for example, in a FISA application, intelligence report, or Section 702 targeting) will assess whether the discrete communication is to, from, or about a tasked selector." Id. The following framework will then be applied:

- If the discrete communication that the analyst seeks to use is to, from, or about a tasked selector, "any U.S. person information in that communication will be handled in accordance with the NSA minimization procedures." Id. Presumably, this means that the discrete communication will be treated as a "foreign communication" that is "of" or "concerning" a United States person, as described above. The MCT containing that communication remains available to analysts in NSA's repositories without any marking to indicate that it has been identified as an MCT or as a transaction containing United States person information.
- If the discrete communication sought to be used is not to, from, or about a tasked selector, and also not to or from an identifiable United States person, "that communication (including any U.S. person information therein) will be handled in accordance with the NSA minimization procedures." Id. at 8-9.⁵² Presumably, this means that the discrete communication will be treated as a "foreign communication" or, if it contains information concerning a United States person, as a "foreign communication" "concerning a United States person," as described above. The MCT itself remains available to analysts in NSA's repositories without any marking to indicate that it has been identified as an MCT or that it contains one or more communications that are not to, from, or about a targeted selector.

⁵¹ A transaction that is identified as an SCT rather than an MCT must be handled in accordance with the standard minimization procedures that are discussed above.

⁵² The Court understands that absent contrary information, NSA treats the user of an account who appears to be located in the United States as "an identifiable U.S. person." See Aug. 30 Submission at 9 n.7 ("To help determine whether a discrete communication not to, from, or about a tasked selector is to or from a U.S. person, NSA would perform the same sort of technical analysis it would perform before tasking an electronic communications account/address/identifier in accordance with its section 702 targeting procedures.").

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

- A discrete communication that is not to, from, or about a tasked selector but that is to or from an identifiable United States person “cannot be used for any purpose other than to protect against an immediate threat to human life (e.g., force protection or hostage situations).” *Id.* at 9. Presumably, this is a reference to Section 1 of the minimization procedures, which allows NSA to deviate from the procedures in such narrow circumstances, subject to the requirement that prompt notice be given to the Office of the Director of National Intelligence, the Department of Justice, and the Court that the deviation has occurred. Regardless of whether or not the discrete communication is used for this limited purpose, the MCT itself remains in NSA’s databases without any marking to indicate that it is an MCT, or that it contains at least one communication that is to or from an identifiable United States person. *See id.*; Sept. 7, 2011 Hearing Tr. at 61.
- If the discrete communication sought to be used by the analyst (or another discrete communication within the MCT) is recognized as being wholly domestic, the entire MCT will be purged from NSA’s systems. *See* Aug. 30 Submission at 3.

c. Statutory Analysis

i. Acquisition

The Court first considers how NSA’s proposed handling of MCTs bears on whether NSA’s minimization procedures are “reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition . . . 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.” *See* 50 U.S.C. § 1801(h)(1) (emphasis added). Insofar as NSA likely acquires approximately 2,000-10,000 MCTs each year that contain at least one wholly domestic communication that is neither to, from, nor about a targeted selector,⁵³ and tens of thousands of communications of or

⁵³ As noted above, NSA’s upstream collection also likely results in the acquisition of tens
(continued...)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

concerning United States persons with no direct connection to any target, the Court has serious concerns. The acquisition of such non-target communications, which are highly unlikely to have foreign intelligence value, obviously does not by itself serve the government's need to "obtain, produce, and disseminate foreign intelligence information." See 50 U.S.C. § 1801(h)(1).

The government submits, however, that the portions of MCTs that contain references to targeted selectors are likely to contain foreign intelligence information, and that it is not feasible for NSA to limit its collection only to the relevant portion or portions of each MCT – i.e., the particular discrete communications that are to, from, or about a targeted selector. The Court

⁵³(...continued)

of thousands of wholly domestic SCTs that contain references to targeted selectors. See supra, pages 33-34 & note 33 (discussing the limits [REDACTED] [REDACTED])

Although the collection of wholly domestic "about" SCTs is troubling, they do not raise the same minimization-related concerns as discrete, wholly domestic communications that are neither to, from, nor about targeted selectors, or as discrete communications of or concerning United States persons with no direct connection to any target, either of which may be contained within MCTs. The Court has effectively concluded that certain communications containing a reference to a targeted selector are reasonably likely to contain foreign intelligence information, including communications between non-target accounts that contain the name of the targeted facility in the body of the message. See Docket No. 07-449, May 31, 2007 Primary Order at 12 (finding probable cause to believe that certain "about" communications were "themselves being sent and/or received by one of the targeted foreign powers"). Insofar as the discrete, wholly domestic "about" communications at issue here are communications between non-target accounts that contain the name of the targeted facility, the same conclusion applies to them. Accordingly, in the language of FISA's definition of minimization procedures, the acquisition of wholly domestic communications about targeted selectors will generally be "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." See 50 U.S.C. 1801(h)(1). Nevertheless, the Court understands that in the event NSA identifies a discrete, wholly domestic "about" communication in its databases, the communication will be destroyed upon recognition. See NSA Minimization Procedures § 5.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

accepts the government's assertion that the collection of MCTs yields valuable foreign intelligence information that by its nature cannot be acquired except through upstream collection. See Sept. 7, 2011 Hearing Tr. at 69-70, 74. For purposes of this discussion, the Court further accepts the government's assertion that it is not feasible for NSA to avoid the collection of MCTs as part of its upstream collection or to limit its collection only to the specific portion or portions of each transaction that contains the targeted selector. See id. at 48-50; June 1 Submission at 27.⁵⁴ The Court therefore concludes that NSA's minimization procedures are, given the current state of NSA's technical capability, reasonably designed to minimize the acquisition 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.

[REDACTED]

In any event, it is incumbent upon NSA to continue working to enhance its capability to limit acquisitions only to targeted communications.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

ii. Retention

The principal problem with the government's proposed handling of MCTs relates to what will occur, and what will not occur, following acquisition. As noted above, the NSA minimization procedures generally require that, "[a]s 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," see NSA Minimization Procedures § 3(b)(4), so that it can be promptly afforded the appropriate treatment under the procedures. The measures proposed by the government for MCTs, however, largely dispense with the requirement of prompt disposition upon initial review by an analyst. Rather than attempting to identify and segregate information "not relevant to the authorized purpose of the acquisition" or to destroy such information promptly following acquisition, NSA's proposed handling of MCTs tends to maximize the retention of such information, including information of or concerning United States persons with no direct connection to any target. See id. § 3(b)(1).

The proposed measures focus almost exclusively on the discrete communications within MCTs that analysts decide, after review, that they wish to use. See Aug. 30 Submission at 8-10. An analyst is not obligated to do anything with other portions of the MCT, including any wholly domestic discrete communications that are not immediately recognized as such, and communications of or concerning United States persons that have no direct connection to the targeted selector. See id.; Sept. 7, 2011 Hearing Tr. at 61. If, after reviewing the contents of an

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

entire MCT, the analyst decides that he or she does not wish to use any discrete communication contained therein, the analyst is not obligated to do anything unless it is immediately apparent to him or her that the MCT contains a wholly domestic communication (in which case the entire MCT is deleted).⁵⁵ See Aug. 30 Submission at 8-10.

Except in the case of those recognized as containing at least one wholly domestic communication, MCTs that have been reviewed by analysts remain available to other analysts in NSA's repositories without any marking to identify them as MCTs. See *id.*; Sept. 7, 2011 Hearing Tr. at 61. Nor will MCTs be marked to identify them as containing discrete communications to or from United States persons but not to or from a targeted selector, or to indicate that they contain United States person information. See Aug. 30 Submission at 8-10; Sept. 7, 2011 Hearing Tr. at 61. All MCTs except those identified as containing one or more wholly domestic communications will be retained for a minimum of five years. The net effect is that thousands of wholly domestic communications (those that are never reviewed and those that are not recognized by analysts as being wholly domestic), and thousands of other discrete

⁵⁵ The government's submissions make clear that, in many cases, it will be difficult for analysts to determine whether a discrete communication contained within an MCT is a wholly domestic communication. NSA's recent manual review of a six-month representative sample of its upstream collection demonstrates how challenging it can be for NSA to recognize wholly domestic communications, even when the agency's full attention and effort are directed at the task. See generally Aug. 16 and Aug. 30 Submissions. It is doubtful that analysts whose attention and effort are focused on identifying and analyzing foreign intelligence information will be any more successful in identifying wholly domestic communications. Indeed, each year the government notifies the Court of numerous compliance incidents involving good-faith mistakes and omissions by NSA personnel who work with the Section 702 collection.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

communications that are not to or from a targeted selector but that are to, from, or concerning a United States person, will be retained by NSA for at least five years, despite the fact that they have no direct connection to a targeted selector and, therefore, are unlikely to contain foreign intelligence information.

It appears that NSA could do substantially more to minimize the retention of information concerning United States persons that is unrelated to the foreign intelligence purpose of its upstream collection. The government has not, for instance, demonstrated why it would not be feasible to limit access to upstream acquisitions to a smaller group of specially-trained analysts who could develop expertise in identifying and scrutinizing MCTs for wholly domestic communications and other discrete communications of or concerning United States persons. Alternatively, it is unclear why an analyst working within the framework proposed by the government should not be required, after identifying an MCT, to apply Section 3(b)(4) of the NSA minimization procedures to each discrete communication within the transaction. As noted above, Section 3(b)(4) states that “[a]s 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.” NSA Minimization Procedures § 3(b)(4). If the MCT contains information “of” or “concerning” a United States person within the meaning of Sections (2)(b) and (2)(c) of the NSA minimization procedures, it is unclear why the analyst should not be required to mark it to identify it as such. At a minimum, it seems that the entire MCT could be marked as an MCT. Such markings would

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

alert other NSA personnel who might encounter the MCT to take care in reviewing it, thus reducing the risk of error that seems to be inherent in the measures proposed by the government, which are applied by each analyst, acting alone and without the benefit of his or her colleagues' prior efforts.⁵⁶ Another potentially helpful step might be to adopt a shorter retention period for MCTs and unreviewed upstream communications so that such information "ages off" and is deleted from NSA's repositories in less than five years.

This discussion is not intended to provide a checklist of changes that, if made, would necessarily bring NSA's minimization procedures into compliance with the statute. Indeed, it may be that some of these measures are impracticable, and it may be that there are other plausible (perhaps even better) steps that could be taken that are not mentioned here. But by not fully exploring such options, the government has failed to demonstrate that it has struck a reasonable balance between its foreign intelligence needs and the requirement that information concerning United States persons be protected. Under the circumstances, the Court is unable to find that, as applied to MCTs in the manner proposed by the government, NSA's minimization procedures are "reasonably designed in light of the purpose and technique of the particular surveillance to minimize the . . . retention . . . of nonpublicly available information concerning unconsenting

⁵⁶ The government recently acknowledged that "it's pretty clear that it would be better" if NSA used such markings but that "[t]he feasibility of doing that [had not yet been] assessed." Sept. 7, 2011 Hearing Tr. at 56.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.”⁵⁷ See 50 U.S.C. §§ 1801(h)(1) & 1821(4)(A).

iii. Dissemination

The Court next turns to dissemination. At the outset, it must be noted that FISA imposes a stricter standard for dissemination than for acquisition or retention. While the statute requires procedures that are reasonably designed to “minimize” the acquisition and retention of information concerning United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information, the procedures must be reasonably designed to “prohibit” the dissemination of information concerning United States persons consistent with that need. See 50 U.S.C. § 1801(h)(1) (emphasis added).

⁵⁷ NSA’s minimization procedures contain two provisions that state, in part, that “[t]he communications that may be retained [by NSA] include electronic communications acquired because of limitations

[REDACTED]. The government further represented that it “ha[d] not seen” such a circumstance in collection under the Protect America Act (“PAA”), which was the predecessor to Section 702. *Id.* at 29, 30. And although NSA apparently was acquiring Internet transactions under the PAA, the government made no mention of such acquisitions in connection with these provisions of the minimization procedures (or otherwise). See *id.* at 27-31. Accordingly, the Court does not read this language as purporting to justify the procedures proposed by the government for MCTs. In any event, such a reading would, for the reasons stated, be inconsistent with the statutory requirements for minimization.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

As the Court understands it, no United States-person-identifying information contained in any MCT will be disseminated except in accordance with the general requirements of NSA's minimization procedures for "foreign communications" "of or concerning United States persons" that are discussed above. Specifically, "[a] report based on communications of or concerning a United States person may be disseminated" only "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." NSA Minimization Procedures § 6(b). A report including the identity of the United States person may be provided to a "recipient requiring the identity of such person for the performance of official duties," but only if at least one of eight requirements is also met – for instance, if "the identity of the United States person is necessary to understand foreign intelligence information or assess its importance." *Id.*⁵⁸

This limitation on the dissemination of United States-person-identifying information is helpful. But the pertinent portion of FISA's definition of minimization procedures applies not merely to information that identifies United States persons, but more broadly to the dissemination of "information concerning unconsenting United States persons." 50 U.S.C. § 1801(h)(1) (emphasis added).⁵⁹ The government has proposed several additional restrictions that

⁵⁸ Although Section 6(b) uses the term "report," the Court understands it to apply to the dissemination of United States-person-identifying information in any form.

⁵⁹ Another provision of the definition of minimization procedures bars the dissemination of information (other than certain forms of foreign intelligence information) "in a manner that
(continued...)"

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

will have the effect of limiting the dissemination of “nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to disseminate foreign intelligence information.” *Id.* First, as noted above, the government will destroy MCTs that are recognized by analysts as containing one or more discrete wholly domestic communications. Second, the government has asserted that NSA will not use any discrete communication within an MCT that is determined to be to or from a United States person but not to, from, or about a targeted selector, except when necessary to protect against an immediate threat to human life. *See* Aug. 30 Submission at 9. The Court understands this to mean, among other things, that no information from such a communication will be disseminated in any form unless NSA determines it is necessary to serve this specific purpose. Third, the government has represented that whenever it is unable to confirm that at least one party to a discrete communication contained in an MCT is located outside the United States, it will not use any information contained in the discrete communication. *See* Sept. 7, 2011 Hearing Tr. at 52. The Court understands this limitation to mean that no information from such a discrete communication will be disseminated by NSA in any form.

Communications as to which a United States person or a person inside the United States

⁵⁹(...continued)

identifies any United States person,” except when the person’s identity is necessary to understand foreign intelligence information or to assess its importance. *See* 50 U.S.C. §§ 1801(h)(2), 1821(4)(b). Congress’s use of the distinct modifying terms “concerning” and “identifying” in two adjacent and closely-related provisions was presumably intended to have meaning. *See, e.g., Russello v. United States*, 464 U.S. 16, 23 (1983).

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

is a party are more likely than other communications to contain information concerning United States persons. And when such a communication is neither to, from, nor about a targeted facility, it is highly unlikely that the “need of the United States to disseminate foreign intelligence information” would be served by the dissemination of United States-person information contained therein. Hence, taken together, these measures will tend to prohibit the dissemination of information concerning unconsenting United States persons when there is no foreign-intelligence need to do so.⁶⁰ Of course, the risk remains that information concerning United States persons will not be recognized by NSA despite the good-faith application of the measures it proposes. But the Court cannot say that the risk is so great that it undermines the reasonableness of the measures proposed by NSA with respect to the dissemination of information concerning United States persons.⁶¹ Accordingly, the Court concludes that NSA’s

⁶⁰ Another measure that, on balance, is likely to mitigate somewhat the risk that information concerning United States persons will be disseminated in the absence of a foreign-intelligence need is the recently-proposed prohibition on running queries of the Section 702 upstream collection using United States-person identifiers. See Aug. 30 Submission at 10-11. To be sure, any query, including a query based on non-United States-person information, could yield United States-person information. Nevertheless, it stands to reason that queries based on information concerning United States persons are at least somewhat more likely than other queries to yield United States-person information. Insofar as information concerning United States persons is not made available to analysts, it cannot be disseminated. Of course, this querying restriction does not address the retention problem that is discussed above.

⁶¹ In reaching this conclusion regarding the risk that information concerning United States persons might be mistakenly disseminated, the Court is mindful that by taking additional steps to minimize the retention of such information, NSA would also be reducing the likelihood that it might be disseminated when the government has no foreign intelligence need to do so.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

minimization procedures are reasonably designed to “prohibit the dissemination[] of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to . . . disseminate foreign intelligence information.” See 50 U.S.C.

§ 1801(h)(1).⁶²

4. NSA’S Targeting and Minimization Procedures Do Not, as Applied to Upstream Collection that Includes MCTs, Satisfy the Requirements of the Fourth Amendment

The final question for the Court is whether the targeting and minimization procedures are, as applied to upstream collection that includes MCTs, consistent with the Fourth Amendment.

See 50 U.S.C. § 1881a(i)(3)(A)-(B). The Fourth Amendment provides:

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.

The Court has assumed in the prior Section 702 Dockets that at least in some circumstances, account holders have a reasonable expectation of privacy in electronic communications, and hence that the acquisition of such communications can result in a “search” or “seizure” within the meaning of the Fourth Amendment. See, e.g., Docket No. [REDACTED]. [REDACTED]. The government accepts the proposition that the acquisition of

⁶² The Court further concludes that the NSA minimization procedures, as the government proposes to apply them to MCTs, satisfy the requirements of 50 U.S.C. §§ 1801(h)(2)-(3) and 1821(4)(B)-(C). See supra, note 59 (discussing 50 U.S.C. §§ 1801(h)(2) & 1821(4)(B)). The requirements of 50 U.S.C. §§ 1801(h)(4) and 1821(4)(D) are inapplicable here.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

electronic communications can result in a “search” or “seizure” under the Fourth Amendment. See Sept. 7, 2011 Hearing Tr. at 66. Indeed, the government has acknowledged in prior Section 702 matters that the acquisition of communications from facilities used by United States persons located outside the United States “must be in conformity with the Fourth Amendment.” Docket Nos. [REDACTED]. The same is true of the acquisition of communications from facilities used by United States persons and others within the United States. See United States v. Verdugo-Urquidez, 494 U.S. 259, 271 (1990) (recognizing that “aliens receive constitutional protections when they have come within the territory of the United States and developed substantial connections with this country”).

a. The Warrant Requirement

The Court has previously concluded that the acquisition of foreign intelligence information pursuant to Section 702 falls within the “foreign intelligence exception” to the warrant requirement of the Fourth Amendment. See Docket No. [REDACTED]. [REDACTED]. The government’s recent revelations regarding NSA’s acquisition of MCTs do not alter that conclusion. To be sure, the Court now understands that, as a result of the transactional nature of the upstream collection, NSA acquires a substantially larger number of communications of or concerning United States persons and persons inside the United States than previously understood. Nevertheless, the collection as a whole is still directed at [REDACTED]. [REDACTED] conducted for the purpose of national security – a

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

purpose going “well beyond any garden-variety law enforcement objective.” See *id.* (quoting *In re Directives*, Docket No. 08-01, Opinion at 16 (FISA Ct. Rev. Aug. 22, 2008) (hereinafter “*In re Directives*”)).⁶³ Further, it remains true that the collection is undertaken in circumstances in which there is a “high degree of probability that requiring a warrant would hinder the government’s ability to collect time-sensitive information and, thus, would impede the vital national security interests that are at stake.” *Id.* at 36 (quoting *In re Directives* at 18). Accordingly, the government’s revelation that NSA acquires MCTs as part of its Section 702 upstream collection does not disturb the Court’s prior conclusion that the government is not required to obtain a warrant before conducting acquisitions under NSA’s targeting and minimization procedures.

b. Reasonableness

The question therefore becomes whether, taking into account NSA’s acquisition and proposed handling of MCTs, the agency’s targeting and minimization procedures are reasonable under the Fourth Amendment. As the Foreign Intelligence Surveillance Court of Review (“Court of Review”) has explained, a court assessing reasonableness in this context must consider “the nature of the government intrusion and how the government intrusion is implemented. The more important the government’s interest, the greater the intrusion that may be constitutionally

⁶³ A redacted, de-classified version of the opinion in *In re Directives* is published at 551 F.3d 1004. The citations herein are to the unredacted, classified version of the opinion.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

tolerated.” In re Directives at 19-20 (citations omitted), quoted in Docket No. [REDACTED]

[REDACTED]. The court must therefore

balance the interests at stake. If the protections that are in place for individual privacy interests are sufficient in light of the government interest at stake, the constitutional scales will tilt in favor of upholding the government’s actions. If, however, those protections are insufficient to alleviate the risks of government error and abuse, the scales will tip toward a finding of unconstitutionality.

Id. at 20 (citations omitted), quoted in Docket No. [REDACTED].

In conducting this balancing, the Court must consider the “totality of the circumstances.” Id. at 19. Given the all-encompassing nature of Fourth Amendment reasonableness review, the targeting and minimization procedures are most appropriately considered collectively. See Docket No. [REDACTED] (following the same approach).⁶⁴

The Court has previously recognized that the government’s national security interest in conducting acquisitions pursuant to Section 702 “is of the highest order of magnitude.” Docket No. [REDACTED] (quoting In re Directives at 20). The Court has further accepted the government’s representations that NSA’s upstream collection is “uniquely capable of acquiring certain types of targeted communications containing valuable foreign intelligence information.” Docket No. [REDACTED] (quoting

⁶⁴ Reasonableness review under the Fourth Amendment is broader than the statutory assessment previously addressed, which is necessarily limited by the terms of the pertinent provisions of FISA.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

government filing). There is no reason to believe that the collection of MCTs results in the acquisition of less foreign intelligence information than the Court previously understood.

Nevertheless, it must be noted that NSA's upstream collection makes up only a very small fraction of the agency's total collection pursuant to Section 702. As explained above, the collection of telephone communications under Section 702 is not implicated at all by the government's recent disclosures regarding NSA's acquisition of MCTs. Nor do those disclosures affect NSA's collection of Internet communications directly from Internet service providers [REDACTED], which accounts for approximately 91% of the Internet communications acquired by NSA each year under Section 702. See Aug. 16 Submission at Appendix A. And the government recently advised that NSA now has the capability, at the time of acquisition, to identify approximately 40% of its upstream collection as constituting discrete communications (non-MCTs) that are to, from, or about a targeted selector. See *id.* at 1 n.2. Accordingly, only approximately 5.4% (40% of 9%) of NSA's aggregate collection of Internet communications (and an even smaller portion of the total collection) under Section 702 is at issue here. The national security interest at stake must be assessed bearing these numbers in mind.

The government's recent disclosures regarding the acquisition of MCTs most directly affect the privacy side of the Fourth Amendment balance. The Court's prior approvals of the targeting and minimization procedures rested on its conclusion that the procedures "reasonably confine acquisitions to targets who are non-U.S. persons outside the United States," who thus

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

“are not protected by the Fourth Amendment.” Docket No. [REDACTED]

[REDACTED] The Court’s approvals also rested upon the understanding that acquisitions under the procedures “will intrude on interests protected by the Fourth Amendment only to the extent that (1) despite the operation of the targeting procedures, U.S. persons, or persons actually in the United States, are mistakenly targeted; or (2) U.S. persons, or persons located in the United States, are parties to communications to or from tasked selectors (or, in certain circumstances, communications that contain a reference to a tasked selector).” *Id.* at 38. But NSA’s acquisition of MCTs substantially broadens the circumstances in which Fourth Amendment-protected interests are intruded upon by NSA’s Section 702 collection. Until now, the Court has not considered these acquisitions in its Fourth Amendment analysis.

Both in terms of its size and its nature, the intrusion resulting from NSA’s acquisition of MCTs is substantial. The Court now understands that each year, NSA’s upstream collection likely results in the acquisition of roughly two to ten thousand discrete wholly domestic communications that are neither to, from, nor about a targeted selector, as well as tens of thousands of other communications that are to or from a United States person or a person in the United States but that are neither to, from, nor about a targeted selector.⁶⁵ In arguing that NSA’s

⁶⁵ As discussed earlier, NSA also likely acquires tens of thousands of discrete, wholly domestic communications that are “about” a targeted facility. Because these communications are reasonably likely to contain foreign intelligence information and thus, generally speaking, serve the government’s foreign intelligence needs, they do not present the same Fourth Amendment concerns as the non-target communications discussed here. *See supra*, note 53.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

targeting and minimization procedures satisfy the Fourth Amendment notwithstanding the acquisition of MCTs, the government stresses that the number of protected communications acquired is relatively small in comparison to the total number of Internet communications obtained by NSA through its upstream collection. That is true enough, given the enormous volume of Internet transactions acquired by NSA through its upstream collection (approximately 26.5 million annually). But the number is small only in that relative sense. The Court recognizes that the ratio of non-target, Fourth Amendment-protected communications to the total number of communications must be considered in the Fourth Amendment balancing. But in conducting a review under the Constitution that requires consideration of the totality of the circumstances, see In re Directives at 19, the Court must also take into account the absolute number of non-target, protected communications that are acquired. In absolute terms, tens of thousands of non-target, protected communications annually is a very large number.

The nature of the intrusion at issue is also an important consideration in the Fourth Amendment balancing. See, e.g., Board of Educ. v. Earls, 536 U.S. 822, 832 (2002); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 659 (1995). At issue here are the personal [REDACTED] communications of U.S. persons and persons in the United States. A person's "papers" are among the four items that are specifically listed in the Fourth Amendment as subject to protection against unreasonable search and seizure. Whether they are transmitted by letter,

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

telephone or e-mail, a person's private communications are akin to personal papers. Indeed, the Supreme Court has held that the parties to telephone communications and the senders and recipients of written communications generally have a reasonable expectation of privacy in the contents of those communications. See Katz, 389 U.S. at 352; United States v. United States Dist. Ct. (Keith), 407 U.S. 297, 313 (1972); United States v. Jacobsen, 466 U.S. 109, 114 (1984). The intrusion resulting from the interception of the contents of electronic communications is, generally speaking, no less substantial.⁶⁶

The government stresses that the non-target communications of concern here (discrete wholly domestic communications and other discrete communications to or from a United States person or a person in the United States that are neither to, from, nor about a targeted selector) are acquired incidentally rather than purposefully. See June 28 Submission at 13-14. Insofar as NSA acquires entire MCTs because it lacks the technical means to limit collection only to the discrete portion or portions of each MCT that contain a reference to the targeted selector, the Court is satisfied that is the case. But as the government correctly recognizes, the acquisition of non-target information is not necessarily reasonable under the Fourth Amendment simply

⁶⁶ Of course, not every interception by the government of a personal communication results in a "search" or "seizure" within the meaning of the Fourth Amendment. Whether a particular intrusion constitutes a search or seizure depends on the specific facts and circumstances involved.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

because its collection is incidental to the purpose of the search or surveillance. See id. at 14.

There surely are circumstances in which incidental intrusions can be so substantial as to render a search or seizure unreasonable. To use an extreme example, if the only way for the government to obtain communications to or from a particular targeted [REDACTED] required also acquiring all communications to or from every other [REDACTED], such collection would certainly raise very serious Fourth Amendment concerns.

Here, the quantity and nature of the information that is “incidentally” collected distinguishes this matter from the prior instances in which this Court and the Court of Review have considered incidental acquisitions. As explained above, the quantity of incidentally-acquired, non-target, protected communications being acquired by NSA through its upstream collection is, in absolute terms, very large, and the resulting intrusion is, in each instance, likewise very substantial. And with regard to the nature of the acquisition, the government acknowledged in a prior Section 702 docket that the term “incidental interception” is “most commonly understood to refer to an intercepted communication between a target using a facility subject to surveillance and a third party using a facility not subject to surveillance.” Docket Nos.

[REDACTED] This is the sort of acquisition that the Court of Review was addressing in In re Directives when it stated that “incidental collections occurring as a result of constitutionally permissible acquisitions do not

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

render those acquisitions unlawful.” In re Directives at 30. But here, by contrast, the incidental acquisitions of concern are not direct communications between a non-target third party and the user of the targeted facility. Nor are they the communications of non-targets that refer directly to a targeted selector. Rather, the communications of concern here are acquired simply because they appear somewhere in the same transaction as a separate communication that is to, from, or about the targeted facility.⁶⁷

The distinction is significant and impacts the Fourth Amendment balancing. A discrete communication as to which the user of the targeted facility is a party or in which the targeted

⁶⁷ The Court of Review plainly limited its holding regarding incidental collection to the facts before it. See In re Directives at 30 (“On these facts, incidentally collected communications of non-targeted United States persons do not violate the Fourth Amendment.”) (emphasis added). The dispute in In re Directives involved the acquisition by NSA of discrete to/from communications from an Internet Service Provider, not NSA’s upstream collection of Internet transactions. Accordingly, the Court of Review had no occasion to consider NSA’s acquisition of MCTs (or even “about” communications, for that matter). Furthermore, the Court of Review noted that “[t]he government assures us that it does not maintain a database of incidentally collected information from non-targeted United States persons, and there is no evidence to the contrary.” Id. Here, however, the government proposes measures that will allow NSA to retain non-target United States person information in its databases for at least five years.

The Title III cases cited by the government (see June 28 Submission at 14-15) are likewise distinguishable. Abraham v. County of Greenville, 237 F.3d 386, 391 (4th Cir. 2001), did not involve incidental overhears at all. The others involved allegedly non-pertinent communications to or from the facilities for which wiretap authorization had been granted, rather than communications to or from non-targeted facilities. See Scott v. United States, 436 U.S. 128, 130-31 (1978), United States v. McKinnon, 721 F.2d 19, 23 (1st Cir. 1983), and United States v. Doolittle, 507 F.2d 1368, 1371, *aff’d en banc*, 518 F.2d 500 (5th Cir. 1975).

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

facility is mentioned is much more likely to contain foreign intelligence information than is a separate communication that is acquired simply because it happens to be within the same transaction as a communication involving a targeted facility. Hence, the national security need for acquiring, retaining, and disseminating the former category of communications is greater than the justification for acquiring, retaining, and disseminating the latter form of communication.

The Court of Review and this Court have recognized that the procedures governing retention, use, and dissemination bear on the reasonableness under the Fourth Amendment of a program for collecting foreign intelligence information. See In re Directives at 29-30; Docket No. [REDACTED]. As explained in the discussion of NSA's minimization procedures above, the measures proposed by NSA for handling MCTs tend to maximize, rather than minimize, the retention of non-target information, including information of or concerning United States persons. Instead of requiring the prompt review and proper disposition of non-target information (to the extent it is feasible to do so), NSA's proposed measures focus almost exclusively on those portions of an MCT that an analyst decides, after review, that he or she wishes to use. An analyst is not required to determine whether other portions of the MCT constitute discrete communications to or from a United States person or a person in the United States, or contain information concerning a United States person or person inside the United States, or, having made such a determination, to do anything about it. Only

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

those MCTs that are immediately recognized as containing a wholly domestic discrete communication are purged, while other MCTs remain in NSA's repositories for five or more years, without being marked as MCTs. Nor, if an MCT contains a discrete communication of, or other information concerning, a United States person or person in the United States, is the MCT marked as such. Accordingly, each analyst who retrieves an MCT and wishes to use a portion thereof is left to apply the proposed minimization measures alone, from beginning to end, and without the benefit of his colleagues' prior review and analysis. Given the limited review of MCTs that is required, and the difficulty of the task of identifying protected information within an MCT, the government's proposed measures seem to enhance, rather than reduce, the risk of error, overretention, and dissemination of non-target information, including information protected by the Fourth Amendment.

In sum, NSA's collection of MCTs results in the acquisition of a very large number of Fourth Amendment-protected communications that have no direct connection to any targeted facility and thus do not serve the national security needs underlying the Section 702 collection as a whole. Rather than attempting to identify and segregate the non-target, Fourth-Amendment protected information promptly following acquisition, NSA's proposed handling of MCTs tends to maximize the retention of such information and hence to enhance the risk that it will be used and disseminated. Under the totality of the circumstances, then, the Court is unable to find that

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

the government's proposed application of NSA's targeting and minimization procedures to MCTs is consistent with the requirements of the Fourth Amendment. The Court does not foreclose the possibility that the government might 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.⁶⁸

V. CONCLUSION

For the foregoing reasons, the government's requests for approval of the certifications and procedures contained in the April 2011 Submissions are granted in part and denied in part. The Court concludes that one aspect of the proposed collection – the “upstream collection” of Internet transactions containing multiple communications, or MCTs – is, in some respects, deficient on statutory and constitutional grounds. Specifically, the Court finds as follows:

1. Certifications [REDACTED] and the amendments to the Certifications in the Prior 702 Dockets, contain all the required elements;

⁶⁸ As the government notes, see June 1 Submission at 18-19, the Supreme Court has “repeatedly refused to declare that only the ‘least intrusive’ search practicable can be reasonable under the Fourth Amendment.” City of Ontario v. Quon, — U.S. —, 130 S. Ct. 2619, 2632 (2010) (citations and internal quotation marks omitted). The foregoing discussion should not be understood to suggest otherwise. Rather, the Court holds only that the means actually chosen by the government to accomplish its Section 702 upstream collection are, with respect to MCTs, excessively intrusive in light of the purpose of the collection as a whole.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

2. As applied to telephone communications and discrete Internet communications that are to or from a facility tasked for collection, to non-MCT “about” communications falling within the [REDACTED] categories previously described by the government,⁶⁹ and to MCTs as to which the “active user” is known to be a tasked selector, the targeting and minimization procedures adopted in accordance with 50 U.S.C. § 1881a(d)-(e) are consistent with the requirements of those subsections and with the Fourth Amendment to the Constitution of the United States;

3. NSA’s targeting procedures, as the government proposes to implement them in connection with the acquisition of MCTs, meet the requirements of 50 U.S.C. § 1881a(d);

4. NSA’s minimization procedures, as the government proposes to apply them to MCTs as to which the “active user” is not known to be a tasked selector, do not meet the requirements of 50 U.S.C. § 1881a(e) with respect to retention; and

5. NSA’s targeting and minimization procedures, as the government proposes to apply them to MCTs as to which the “active user” is not known to be a tasked selector, are inconsistent with the requirements of the Fourth Amendment.

⁶⁹ See Docket No. [REDACTED].

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Orders approving the certifications and amendments in part are being entered contemporaneously herewith.

ENTERED this 3rd day of October, 2011.



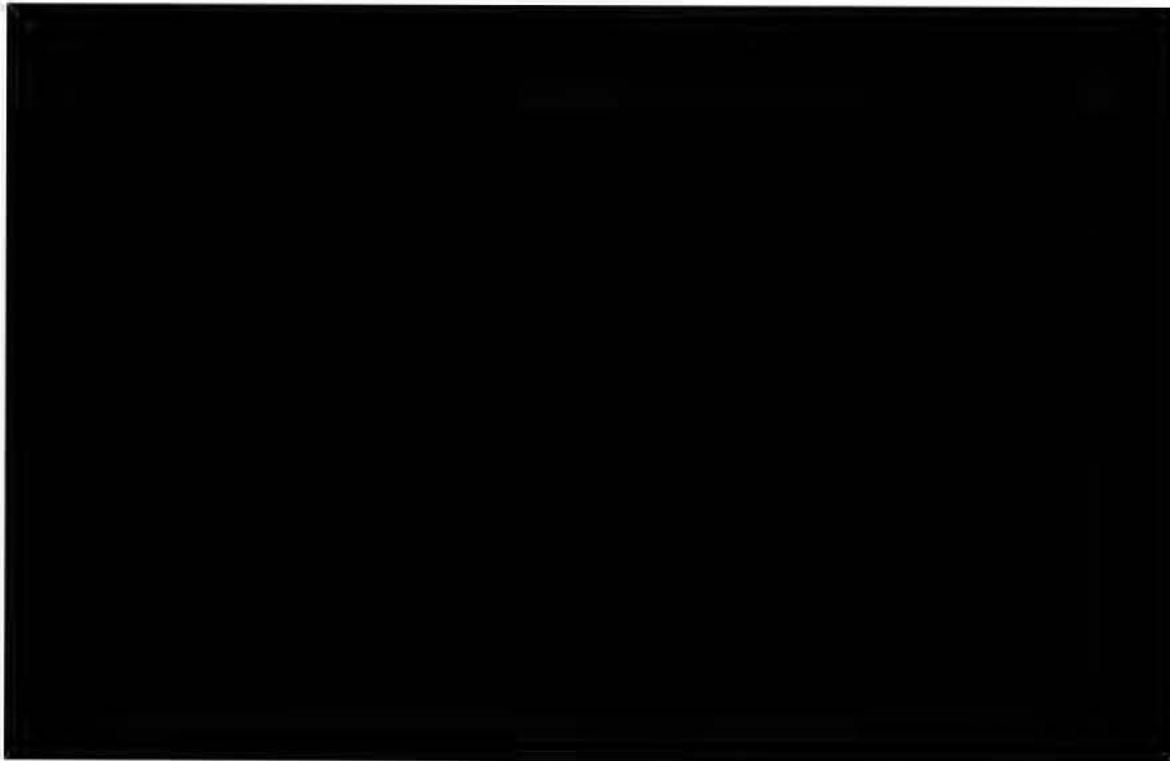
JOHN D. BATES
Judge, United States Foreign
Intelligence Surveillance Court

~~TOP SECRET//COMINT//ORCON,NOFORN~~

██████████, Deputy Clerk,
FISC, certify that this document
is a true and correct copy of
the original. ██████████

~~TOP SECRET//COMINT//ORCON,NOFORN~~

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.



ORDER

These matters are before the Court on: (1) the "Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications" for DNI/AG 702(g) Certifications [REDACTED], which was filed

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

on April 20, 2011; (2) the “Government’s Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications” for DNI/AG 702(g) Certifications [REDACTED], which was filed on April 22, 2011; and (3) the “Government’s Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications” for DNI/AG 702(g) Certifications [REDACTED], which was also filed on April 22, 2011 (collectively, the “April 2011 Submissions”).

Through the April 2011 Submissions, the government seeks approval of the acquisition of certain telephone and Internet communications pursuant to Section 702 of the Foreign Intelligence Surveillance Act (“FISA” or the “Act”), 50 U.S.C. § 1881a, which requires judicial review for compliance with both statutory and constitutional requirements. For the reasons set forth in the accompanying Memorandum Opinion, the government’s requests for approval are granted in part and denied in part. The Court concludes that one aspect of the proposed collection – the “upstream collection” of Internet transactions containing multiple communications, or “MCTs” – is, in some respects, deficient on statutory and constitutional grounds. Specifically, the Court finds as follows:

1. DNI/AG 702(g) Certifications [REDACTED], as well as the amendments to the other certifications listed above and contained in the April 2011 Submissions,

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

contain all the required elements;

2. As applied to telephone communications and discrete Internet communications that are to or from a facility tasked for collection, to non-MCT “about” communications falling within the [REDACTED] categories previously described by the government,¹ and to MCTs as to which the “active user” is known to be a tasked selector, the targeting and minimization procedures adopted in accordance with 50 U.S.C. § 1881a(d)-(e) are consistent with the requirements of those subsections and with the Fourth Amendment to the Constitution of the United States;

3. NSA’s targeting procedures, as the government proposes to implement them in connection with the acquisition of MCTs, meet the requirements of 50 U.S.C. § 1881a(d);

4. NSA’s minimization procedures, as the government proposes to apply them to MCTs as to which the “active user” is not known to be a tasked selector, do not meet the requirements of 50 U.S.C. § 1881a(e) with respect to retention; and

5. NSA’s targeting and minimization procedures, as the government proposes to apply them to MCTs as to which the “active user” is not known to be a tasked selector, are inconsistent with the requirements of the Fourth Amendment.

Accordingly, pursuant to 50 U.S.C. § 1881a(i)(3)(B), the government shall, at its election:

(a) not later than 30 days from the issuance of this Order, correct the deficiencies identified in the accompanying Memorandum Opinion; or,

¹ See Docket No. 702(i)-08-01, Sept. 4, Memorandum Opinion at 17-18 n.14.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~



(b) cease the implementation of the Certifications insofar as they permit the acquisition of MCTs as to which the "active user" is not known to be a tasked selector.

ENTERED this 3rd day of October, 2011, at 4:55 p.m. Eastern Time.



JOHN D. BATES
Judge, United States Foreign
Intelligence Surveillance Court

~~TOP SECRET//COMINT//ORCON,NOFORN~~

I,  Deputy Clerk,
FISC, certify that this document
is a true and correct copy of
the original. 

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 17

IC ON THE RECORD

- Section 702 Overview
-  CY2017 Transparency Report
- CY2016 SIGNALS INTEL REFORM REPORT
- IC TRANSPARENCY PLAN



DNI Declassifies Intelligence Community Documents Regarding Collection Under Section 702 of the Foreign Intelligence Surveillance Act (FISA)

Wednesday, August 21, 2013

In June, President Obama requested that Director of National Intelligence James R. Clapper declassify and make public as much information as possible about certain sensitive NSA programs while being mindful of the need to protect sensitive classified intelligence and national security.

Consistent with this directive and in the interest of increased transparency, DNI Clapper has today authorized the declassification and public release of a number of documents pertaining to the Intelligence Community's collection under Section 702 of the Foreign Intelligence Surveillance Act (FISA). DNI Clapper has determined that the release of these documents is in the public interest.

These documents and other unclassified information related to foreign intelligence surveillance activities are available on a new Intelligence Community website established at the direction of the President. The new www.icontherecord.tumblr.com is designed to provide immediate, ongoing and direct access to factual information related to the lawful foreign surveillance activities carried out by the U.S. Intelligence Community.

The Administration is undertaking a careful and thorough review of whether and to what extent additional information or documents pertaining to this program may be declassified, consistent with the protection of national security. *IC on the Record* provides a single online location to access new information as it is made available from across the Intelligence Community.

Shawn Turner
Director of Public Affairs
Office of the Director of National Intelligence

Documents being released today include:

[DNI James Clapper's Cover Letter Announcing the Document Release](#)

[October 3, 2011 – Foreign Intelligence Surveillance Court Memorandum Opinion and Order \(J. Bates\)](#) *

[November 30, 2011 – Foreign Intelligence Surveillance Court Memorandum Opinion and Order \(J. Bates\) - Part 1 | Part 2](#)

[September 25, 2012 – Foreign Intelligence Surveillance Court Memorandum Opinion and Order \(J. Bates\)](#)

[December 8, 2011 — Lisa Monaco, John C. \(“Chris”\) Inglis, Robert Litt - Statement for the Record before the House Permanent Select Committee on Intelligence](#)

[February 9, 2012 — Lisa Monaco, John C. \(“Chris”\) Inglis, Robert Litt - Statement for the Record before the House Permanent Select Committee on Intelligence](#)

[May 4, 2012 — Letters to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence Leadership regarding Section 702 Congressional White Paper entitled The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act](#)

JA2718

12/17/2018

ICON THE RECORD • DNI Declassifies Intelligence Community Documents...

Case 1:15-cv-00662-TSE Document 168-21 Filed 12/18/18 Page 3 of 4

October 31, 2011 — Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702, as amended

August 2013 — Semi-Annual Assessment of Compliance with the 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

June 19, 2017 NYT FOIA Release Documents

- [Motion for Secondary Orders **](#)
- [Motion to Extend Time **](#)
- [November 7, 2011 Order **](#)
- [FISC Questions Regarding Amended 2011 Section 702 Certifications **](#)

September 13, 2017 NYT FOIA Release Documents

- [Govt Clarification of NSA Upstream Collection dated May 2, 2011](#)
- [FISC Briefing Order dated May 2011](#)
- [FISC Section 702 Order dated 2011](#)
- [FISC Hearing Transcript dated Sep. 7, 2011](#)
- [Govt Letter to FISC with Additional Information re 702 dated Sep. 9, 2011](#)
- [Govt Supplement Letter to FISC dated Sep. 13, 2011](#)
- [FISC Section 702 Order dated Sep. 14, 2011](#)
- [FISC Briefing Order dated Oct. 13, 2011](#)
- [Govt Preliminary Notice of Compliance Incidents dated Apr. 19, 2011](#)
- [FISC Order dated 2011](#)
- [Govt Motion for Secondary Orders dated Oct. 4, 2011](#)
- [Notice of Filing of Govt Responses to FISC Questions dated Nov 15 2011](#)

October 11, 2017 NYT FOIA Release Documents

- [Motion to Extend Time Limits dated May 5, 2011](#)
- [Government's Reauthorization Certification and Related Documents dated Apr. 22, 2011](#)
- [Follow-Up Questions Regarding Section 702 Certifications dated Jun. 17, 2011](#)
- [Government's Response to May 9, 2011 Briefing Order dated Jun. 1, 2011](#)
- [Motion to Extend Time Limits dated Jul. 14, 2011](#)
- [Government's Supplement to June 1 and June 28, 2011 Submissions dated Aug. 16, 2011](#)
- [Government's Amendment to Section 702 Certification and Amended Minimization Procedures dated Oct. 31, 2011](#)
- [Government's Notice of Clarifications dated Aug. 16, 2011](#)
- [Government's Response to October 13, 2011 Briefing Order dated Nov. 22, 2011](#)
- [Government's Request for Issuance of Notices dated Oct. 31, 2011](#)
- [Government's Notice dated Nov. 29, 2011](#)

* Updated 07/16/14 to reflect additional declassification concerning the now-discontinued NSA bulk electronic communications metadata program.

** Updated 6/19/17 to reflect additional declassification concerning the now-discontinued NSA bulk electronic communications metadata program.

- [#Declassified](#)
- [#Section 702](#)
- [#FISA](#)
- [#NSA](#)
- [5 years ago](#)
- [194](#)
- [Permalink](#)

Share

Short URL

<https://tumblr.co/ZZQjsqsvMU>

[Twitter](#)[Facebook](#)[Pinterest](#)[Google+](#)

194 Notes/ [Show](#)

← Previous • Next →

JA2719

IC ON THE RECORD:

Direct access to factual information related to the lawful foreign surveillance activities of the U.S. Intelligence Community.

Created at the direction of the President of the United States and maintained by the Office of the Director of National Intelligence.

[Guide to Posted Documents Regarding Use of National Security Authorities](#)

CONTENT:

- - [Official Statements](#)
- - [Declassified Documents](#)
- - [Testimony](#)
- - [Speeches & Interviews](#)
- - [Fact Sheets](#)
- - [Oversight & Compliance](#)
- - [Video](#)
- - [IC Budget](#)

HOT TOPICS:

- - [Civil Liberties](#)
- - [FISA](#)
- - [FISC](#)
- - [Section 215](#)
- - [Section 702](#)

THEIR OWN WORDS:

- - [Mike Rogers, Dir. NSA](#)
- - [Rick Ledgett, Dep. Dir. NSA](#)
- - [Alex Joel, CLPT, ODNI](#)
- - [Becky Richards, CLPO, NSA](#)

(Former IC Officials)

- - [James Clapper, DNI](#)
- - [Keith Alexander, Dir. NSA](#)
- - [John Inglis, Dep. Dir. NSA](#)
- - [Robert Litt, GC, ODNI](#)
- - [Rajesh De, GC, NSA](#)
- - [John DeLong, CD, NSA](#)



This website is maintained by the [Office of the Director of National Intelligence](#).

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 18

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

WIKIMEDIA FOUNDATION,)	
)	
Plaintiff,)	
)	
v.)	No. 1:15-cv-00662-TSE
)	
NATIONAL SECURITY AGENCY, <i>et al.</i> ,)	
)	
Defendants.)	

**OBJECTIONS AND RESPONSES BY DEFENDANTS NATIONAL
SECURITY AGENCY AND ADM. MICHAEL S. ROGERS,
DIRECTOR, TO PLAINTIFF’S INTERROGATORIES**

Pursuant to Rule 33 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 Interrogatories, dated November 7, 2017.

**GENERAL OBJECTIONS AND
OBJECTIONS TO DEFINITIONS AND INSTRUCTIONS**

1. The NSA Defendants object to Plaintiff’s Interrogatories to the extent, as set forth in response to specific interrogatories below, that they seek information regarding the activities of the NSA, which is absolutely protected from disclosure by the statutory privilege under 50 U.S.C. § 3605(a).

2. The NSA Defendants object to Plaintiff’s Interrogatories to the extent, as set forth in response to specific interrogatories 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.

3. As set forth in response to each interrogatory below, the NSA Defendants object to the definition the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

4. As set forth in response to specific interrogatories 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 interrogatories 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 interrogatories below, the NSA Defendants object to the definition of the term “Review” as compound, unduly burdensome and oppressive,

and so vague and ambiguous as to render the specific interrogatories in which it is used incapable of reasoned response.

7. As set forth in response to specific interrogatories below, the NSA Defendants object to the definition of the term “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 the specific interrogatories in which it is used incapable of reasoned response.

8. As set forth in response to specific interrogatories below, the NSA Defendants object to Plaintiff’s Interrogatories 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. As set forth in response to specific interrogatories below, the NSA Defendants object to Instruction No. 3 in Plaintiff’s Interrogatories to the extent that identification or description of each document or oral communication as to which privilege is claimed would itself divulge privileged information.

10. The NSA Defendants object to Plaintiff’s Interrogatories to the extent that they seek information not involving the NSA’s Upstream Internet acquisition techniques as authorized by Section 702 of the Foreign Intelligence Surveillance Act (“FISA”), 50 U.S.C. § 1881a. In formulating these answers, the NSA Defendants have limited the scope of their inquiry of knowledgeable persons, as well as their searches of appropriate records, to those persons and records reasonably calculated to possess information involving the NSA’s Upstream Internet acquisition techniques as authorized by Section 702 of the FISA.

11. 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.

12. Nothing contained in the following objections and responses shall be construed as a waiver of any applicable objection or privilege as to any interrogatory 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 INTERROGATORIES

INTERROGATORY NO. 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.

OBJECTION: The NSA Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 1 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants also object to Interrogatory No. 1 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 Interrogatory No. 1 on the grounds that the instruction to “provide all information supporting [their] understanding [of the definition of the

term ‘international Internet link’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 1 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 1 on the ground that it seeks information 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

INTERROGATORY NO. 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.

OBJECTION: The NSA Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 2 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants also object to Interrogatory No. 2 on the grounds that the instruction to “provide all information supporting [their] understanding [of the definition of the term ‘circuit’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

The NSA Defendants further object to this interrogatory on the ground that 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.

Finally, to the extent that Interrogatory No. 2 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 2 on the grounds that it seeks information 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the 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.

As of the time of this response the NSA Defendants are unaware of any information furnished by Defendants to the PCLOB regarding the meaning of the term “circuit” that would differ from the understanding set forth above.

INTERROGATORY NO. 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.

OBJECTION: The NSA Defendants object to the definition the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 3 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 3 on the grounds that the instruction to “provide all information supporting [their] understanding [of the definition of the term ‘filtering mechanism’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 3 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 3 on the grounds that it seeks information 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the 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.

INTERROGATORY NO. 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.

OBJECTION: The NSA Defendants object to the definition the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 4 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 4 on the grounds that the instruction to “provide all information supporting [their] understanding [of the definition of the term ‘scanned’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 4 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 4 on the grounds that it seeks information 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that to their understanding the term “scanned,” as used in the above-referenced brief when filed, meant, in unclassified terms, the use of a screening device in the Upstream Internet collection process to acquire only Internet transactions containing at least one tasked selector. Today the term “scanned” would mean, in unclassified terms, the use of a screening device in the Upstream Internet collection process designed to identify for acquisition Internet transactions to or from persons targeted in accordance with the current NSA targeting procedures.

INTERROGATORY NO. 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.

OBJECTION: The NSA Defendants object to the definition the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 5 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 5 on the grounds that its instruction to “provide all information supporting [their] understanding [of the definition of the term ‘screen’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 5 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 5 on the grounds that it seeks information 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

object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that to their understanding the term “screen,” as used in the above-referenced brief when filed, meant, in unclassified terms, the use of a screening device in the Upstream Internet collection process to acquire only Internet transactions containing at least one tasked selector. Today, the term “screened” would mean, in unclassified terms, the use of a screening device in the Upstream Internet collection process designed to identify for acquisition Internet transactions to or from persons targeted in accordance with the current NSA targeting procedures.

INTERROGATORY NO. 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.

OBJECTION: The NSA Defendants object to Interrogatory No. 6 on the grounds that 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. The NSA Defendants also object to the definition the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 6 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 6 on the grounds that the instruction to “provide all information supporting [their] understanding [of the definition of the

term ‘discrete communication’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 6 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 6 on the grounds that it seeks information 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, in the context of the 2014 NSA Section 702 Minimization Procedures, the term “discrete communication” means a single communication.

INTERROGATORY NO. 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).

OBJECTION: NSA Defendants object to the definition the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 7 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 7 on the grounds that its instruction to “provide all information supporting [their] understanding [of the ‘features that a

series of Internet packets comprising an “Internet transaction” has in common’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, the NSA Defendants object to Interrogatory No. 7 on the ground that it seeks classified information about alleged NSA intelligence activities 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

INTERROGATORY NO. 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).

OBJECTION: The NSA Defendants object to Interrogatory No. 8 on the grounds that 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. The NSA Defendants also object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 8 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants also object to Interrogatory No. 8 as vague and ambiguous insofar as it attributes the phrase “single communication transaction” 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 *9 (FISC Oct. 3, 2011).

The NSA Defendants further object to Interrogatory No. 8 on the grounds that its instruction to “provide all information supporting [their] understanding [of the terms ‘single communication transaction’ and ‘multi-communication transaction’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 8 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 8 on the grounds that it seeks information 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the 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-communication transaction” meant, in unclassified terms, an Internet transaction that contained multiple discrete communications.

INTERROGATORY NO. 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.

OBJECTION: The NSA Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 9 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 9 on the grounds that its instruction to “provide all information supporting [their] understanding [of the terms ‘access’ and ‘larger body of international communications’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 9 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 9 on the grounds that it seeks information 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that to their understanding (i) the term “larger body of international communications,” as used in the above-referenced brief when filed, meant, in unclassified terms, the body of at least one-end-foreign Internet transactions transiting the Internet backbone networks of electronic communications service providers that were screened during the

Upstream Internet collection process for the purpose of identifying those containing at least one tasked selector; and (ii) the term “access,” as used in the same brief when filed, referred in unclassified terms to the means making it possible to screen this “larger body of international communications” for those that contained at least one tasked selector. As noted above in response to Interrogatory Nos. 3-5, today Internet transactions are screened during the Upstream Internet collection process to identify for acquisition those transactions that are to or from persons targeted in accordance with the current NSA targeting procedures.

INTERROGATORY NO. 10: DESCRIBE YOUR understanding of the definition of the term “acquired” 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.

OBJECTION: The NSA Defendants object to the definition the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 10 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 10 on the grounds that its instruction to “provide all information supporting [their] understanding [of the term ‘acquired’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 10 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 10 on the grounds that it seeks information 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify

and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that to their understanding the term “acquired,” as used in the above-referenced brief in relation to Internet transactions, meant when filed (and still means today), in unclassified terms, ingested into Government databases after the Internet transactions have passed through the filtering and scanning processes conducted during Upstream Internet collection.

INTERROGATORY NO. 11: DESCRIBE YOUR understanding of the definition of the term “collection” as used 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.

OBJECTION: The NSA Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 11 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 11 on the grounds that its instruction to “provide all information supporting [their] understanding [of the term ‘collection’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 11 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 11 on the grounds that it seeks information 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

object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that to their understanding the term “collection,” as used in the above-referenced brief in relation to communications, meant when filed (and still means today), in unclassified terms, ingestion into Government databases after Internet transactions have passed through the filtering and scanning processes conducted during Upstream Internet collection.

INTERROGATORY NO. 12: DESCRIBE YOUR understanding of the definition of the term “Internet ‘backbone’” as used at page 1 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.

OBJECTION: The NSA Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 12 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 12 on the grounds that its instruction to “provide all information supporting [their] understanding [of the term ‘Internet ‘backbone’]” is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 12 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 12 on the grounds that it seeks information 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

object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the 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.

INTERROGATORY NO. 13: DESCRIBE in detail all steps taken by the NSA to PROCESS communications in the course of Upstream surveillance.

OBJECTION: The NSA Defendants object to Interrogatory No. 13 on the grounds that 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. The NSA Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 13 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

Finally, the NSA Defendants object to Interrogatory No. 13 on the ground that it seeks information about alleged NSA intelligence activities 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 object to any instruction or purported requirement, *see* Fed. R.

Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

INTERROGATORY NO. 14: DESCRIBE the entire process by which, pursuant to Upstream surveillance, the contents of INTERNET COMMUNICATIONS are INTERACTED WITH.

OBJECTION: The NSA Defendants object to the definition of the term “Describe” to the extent it calls for “identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants’ narrative statement]” in response to Interrogatory No. 14 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous. The NSA Defendants also 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 this interrogatory incapable of reasoned response.

The NSA Defendants further object to Interrogatory No. 14 to the extent grounds that 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.

Finally, the NSA Defendants object to Interrogatory No. 14 on the ground that it seeks information about alleged NSA intelligence activities 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

Dated: December 22, 2017

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
CAROLINE J. ANDERSON
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

Pursuant to 28 U.S.C. § 1746, I, Jason D. Padgett, declare under penalty of perjury that the foregoing answers to Plaintiff Wikimedia's Interrogatories are true and correct to the best of my knowledge and belief, based on my personal knowledge and information made available to me in the course of my duties and responsibilities as an Attorney in the Office of General Counsel, National Security Agency.

Executed this 22nd day of December, 2017



Jason D. Padgett
Attorney
Office of General Counsel
National Security Agency

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 19

All withheld information exempt under b(1) and b(3) unless otherwise noted.

Approved for public release.



U.S. Department of Justice

National Security Division

U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT

2011 MAY -2 AM 11:48

~~TOP SECRET//COMINT//NOFORN~~

Washington, D.C. 20530

LEEANN FLYNN HALL
CLERK OF COURT

May 2, 2011

The Honorable John D. Bates
United States Foreign Intelligence Surveillance Court
333 Constitution Avenue, N.W.
Washington, D.C. 20001

Re: Clarification of National Security Agency's
Upstream Collection Pursuant to Section 702 of
FISA ~~(S//SI//NF)~~

Dear Judge Bates:

On April 21, 2011, the National Security Agency (NSA) provided the National Security Division (NSD) and the Office of the Director of National Intelligence (ODNI) information clarifying the manner in which NSA acquires certain communications through its upstream collection platforms pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended (FISA). Although NSA, NSD, and ODNI are still reviewing this matter and assessing its import, we are providing preliminary notice at this time pursuant to Rule 13(a) of the Rules of Procedure for the Foreign Intelligence Surveillance Court, effective November 1, 2010, in order provide the Court with this additional clarifying information. We have worked closely in these efforts with NSA officials, who have assisted in drafting and reviewing this notice to the Court. ~~(TS//SI//NF)~~

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. The term "Internet communications," as described by the Director of NSA in affidavits supporting DNI/AG 702(g) certifications, "is intended to include electronic communications that



702(g) Certification
Director, NSA, filed

2010, ¶ 6.

Affidavit of General Keith B. Alexander,
Sec. e.g., DNI/AG

~~TOP SECRET//COMINT//NOFORN~~

~~Classified by: Tashina Gauhar, Deputy Assistant
Attorney General, NSD, DOJ~~

~~Reason: 1.4(c)~~

~~Declassify on: May 2, 2036~~

OI Tracking No. 104876

All withheld information exempt under b(1) and b(3) unless otherwise noted.

Approved for public release.

~~TOP SECRET//COMINT//NOFORN~~

[REDACTED]

[REDACTED]

[REDACTED] (TS//SI//NF)

In past representations to the Court, the Government used as an example of upstream collection the acquisition of [REDACTED] that contained a selector that NSA had tasked under Section 702, such that NSA acquired the [REDACTED] while it was being transmitted to or from a user of the non-tasked account.¹

Based on recent discussions among NSA, NSD, and ODNI regarding one specified category of Internet communications acquired through upstream collection—"electronic communications [REDACTED]"—and in view of the complexity of this issue and the prior representations to the Court, the Government believes that further description of the scope of NSA's upstream collection is warranted. (TS//SI//NF)

One type of "electronic communications [REDACTED]"

[REDACTED]

[REDACTED] (TS//SI//NF)

Depending on [REDACTED], the data transmitted [REDACTED] may also include [REDACTED]

¹ [REDACTED] (TS//SI//NF)

² [REDACTED] (TS//SI//NF)

~~TOP SECRET//COMINT//NOFORN~~

All withheld information exempt under b(1) and b(3) unless otherwise noted.

Approved for public release.

~~TOP SECRET//COMINT//NOFORN~~

[REDACTED] including e-mail messages that are not to, from, or about a Section 702-targeted individual. For example, [REDACTED]

[REDACTED] The content of [REDACTED]

[REDACTED] would be acquired through NSA's Section 702 upstream collection if a tasked selector appeared anywhere [REDACTED]

[REDACTED] (TS//SI//NF)

As this example demonstrates, an individual Internet communication can contain a single piece of information [REDACTED], or it could contain multiple pieces of information [REDACTED]

[REDACTED] (TS//SI//NF)

Additionally, as described in the NSA's targeting procedures, "in those cases where NSA seeks to acquire communications about the target that are not to or from the target, NSA will employ either an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas, or [REDACTED] See, e.g., DNI/AG 702(g) Certification [REDACTED] Exhibit A at 2. It is through these measures that NSA prevents the intentional acquisition of Internet communications that contain a reference to a targeted selector where the sender and all intended recipients are known at the time of acquisition to be located in the United States. See, e.g., In re DNI/AG Certification [REDACTED] No. 702(i)-08-01, Mem. Op. at 19 (USFISC Sept. 4, 2008). NSA, NSD, and ODNI are continuing to examine what affect, if any, the type of Internet communications collection discussed in this letter has on the efficacy of these measures.

(TS//SI//NF)

~~TOP SECRET//COMINT//NOFORN~~

All withheld information exempt under b(1) and b(3) unless otherwise noted.

Approved for public release.

~~TOP SECRET//COMINT//NOFORN~~

NSA, NSD, and ODNI are continuing to review and assess this matter and will provide additional information to the Court as appropriate. We appreciate the Court's consideration of this matter and welcome additional opportunities to present further information to the Court.

~~(TS//SI//NF)~~

Respectfully submitted, 



Office of Intelligence, NSD
U.S. Department of Justice

~~TOP SECRET//COMINT//NOFORN~~

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 20

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE



STATISTICAL TRANSPARENCY REPORT
Regarding Use of National Security Authorities
~ Calendar Year 2017 ~

LEADING INTELLIGENCE INTEGRATION

Office of Civil Liberties, Privacy, and Transparency
April 2018

STATISTICAL TRANSPARENCY REPORT
Regarding Use of National Security Authorities
~ Calendar Year 2017 ~

Table of Contents

- Introduction 3
 - A. Background. 3
 - B. Areas Covered in this Report. 4
 - C. Context and Clarity. 5
 - D. Key Terms..... 5
- FISA Probable Cause Authorities 7
 - A. FISA Titles I and III 7
 - B. FISA Title VII, Sections 703 and 704..... 7
 - C. Statistics 8
- FISA Section 702..... 10
 - A. Section 702..... 10
 - B. Statistics—Orders and Targets 12
 - C. Statistics—U.S. Person Queries 14
 - D. Section 702 and FBI Investigations. 19
- NSA Dissemination of U.S. Person Information under FISA Section 702 20
 - A. Section 702..... 20
 - B. Statistics 22
- FISA Criminal Use and Notice Provisions 25
 - A. FISA Sections 106 and 305 25
 - B. Statistics 25
- FISA Title IV – Use of Pen Register and Trap and Trace (PR/TT) Devices 27
 - A. FISA Pen Register/Trap and Trace Authority. 27
 - B. Statistics 27
- FISA Title V – BUSINESS RECORDS 30
 - A. Business Records FISA..... 30
 - B. Statistics – “Traditional” Business Records Statistics Orders, Targets & Identifiers 31
 - C. Statistics – Call Detail Record (CDR) Orders, Targets & Identifiers 32
 - D. Statistics – Call Detail Records Queries 35
- NATIONAL SECURITY LETTERS (NSLs)..... 36
 - A. National Security Letters..... 36
 - B. Statistics – National Security Letters and Requests of Information 36
- APPENDIX A..... 39

Introduction

Today, consistent with the USA FREEDOM Act and the FISA Amendments Reauthorization Act of 2017 (the reauthorized FAA) requirements to release certain statistics (codified in 50 U.S.C. § 1873(b)) and the Intelligence Community's (IC) [Principles of Intelligence Transparency](#), we are releasing our **fifth** annual *Statistical Transparency Report Regarding Use of National Security Authorities* presenting statistics on how often the government uses certain national security authorities. Providing these statistics allows for an additional way to track the use of Foreign Intelligence Surveillance Act (FISA) authorities and gives further context to the IC's rigorous and multi-layered oversight framework that safeguards the privacy of United States person information acquired pursuant to FISA. The report goes beyond its statutory duty of providing statistics and further provides the public with detailed explanation as to how the IC uses these national security authorities.

Additional public information on national security authorities is available at the Office of the Director of National Intelligence's (ODNI) website, www.dni.gov, and ODNI's public tumblr site, [IC on the Record](#). Furthermore, since the release of the previous report, ODNI has created the new website, www.intelligence.gov, that contains additional public information on the IC's activities.

A. Background.

In June [2014](#), the Director of National Intelligence (DNI) began releasing statistics relating to the use of critical national security authorities, including the FISA, in an annual report called the *Statistical Transparency Report Regarding Use of National Security Authorities* (hereafter the *Annual Statistical Transparency Report*). Subsequent *Annual Statistical Transparency Reports* were released in [2015](#), [2016](#), and [2017](#).

On June 2, 2015, the USA FREEDOM Act was enacted, codifying a requirement to publicly report many of the statistics already reported in the *Annual Statistical Transparency Report*. The Act also expanded the scope of the information included in the reports by requiring the DNI to report information concerning United States person (U.S. person or USP) search terms and queries of certain FISA-acquired information, as well as specific statistics concerning call detail records. See 50 U.S.C. § 1873(b). On January 19, 2018, the reauthorized FAA was signed. See 50 U.S.C. § 1881a. The reauthorized FAA (also referred to as the Section 702 Reauthorization Act of 2017) codified additional statistics that must be publicly released, including many statistics that the government previously reported pursuant to its commitment to transparency.

B. Areas Covered in this Report.

This report provides statistics in the following areas (the terms used below are defined and explained later in this report):

- **FISA Probable Cause Authorities.** The number of orders—and the number of targets under those orders—for the use of FISA authorities that require probable cause determinations by the Foreign Intelligence Surveillance Court (FISC), under Titles I and III, and Section 703 and 704, of FISA.
- **FISA Section 702.**
 - The number of orders—and the number of targets under those orders—issued pursuant to Section 702 of FISA.
 - The number of U.S. person queries of Section 702-acquired content and metadata.
 - The number of instances in which the Federal Bureau of Investigation (FBI) personnel received and reviewed Section 702-acquired information that the FBI identified as concerning a U.S. person in response to a query that was designed to return evidence of a crime unrelated to foreign intelligence.
 - The number of instances in which the FBI opened, under the Criminal Investigative Division, an investigation of a U.S. person (who is not considered a threat to national security) based wholly or in part on Section 702-acquired information.
 - The number of National Security Agency (NSA)-disseminated Section 702 reports containing U.S. person identities (various statistics relating to reports where the U.S. person identity was openly named or originally masked and subsequently unmasked).
- **Use in Criminal Proceedings.** The number of criminal proceedings in which the United States or a State or political subdivision provided notice under FISA of the government's intent to enter into evidence or otherwise use or disclose any information derived from electronic surveillance, physical search, or Section 702 acquisition.
- **Pen Register and Trap and Trace Devices.** The number of orders—and the number of targets under those orders—for the use of FISA's pen register/trap and trace devices, and the number of unique identifiers used to communicate information collected pursuant to those orders.
- **Business Records.** The number of orders—and the number of targets under those orders—issued pursuant to FISA's business records authority, and the number of unique identifiers used to communicate information collected pursuant to those orders. In

addition, the number of orders—and the number of targets under those orders—issued pursuant to FISA’s business record authority for the production of call detail records, and the number of call detail records received from providers and stored in NSA repositories.

- **National Security Letters.** The number of national security letters issued, and the number of requests for information within those national security letters.

C. Context and Clarity.

[Consistent with the IC’s Principles of Intelligence Transparency](#), this report seeks to enhance public understanding by including explanations and charts for context and clarity. For example, the report provides charts that place the statistics in this report in context with the statistics in prior reports. While these statistics provide an important point of reference for understanding the use of these authorities, it is important to keep in mind the statistics’ limitations. The statistics fluctuate from year to year for a variety of reasons (e.g., operational priorities, world events, technical capabilities), some of which cannot be explored in an unclassified setting. Moreover, there may be no relationship between a decrease in the use of one authority and an increase in another. Nonetheless, we believe this report provides helpful information about how the IC uses these vital national security authorities.

D. Key Terms.

Certain terms used throughout this report are described below. Other terms are described in the sections in which they are most directly relevant.

- **U.S. Person.** As defined by Title I of FISA, a U.S. person is “a citizen of the United States , an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in [50 U.S.C. § 1801(a)(1), (2), or (3)].” 50 U.S.C. § 1801(i). Section 602 of the USA FREEDOM Act, however, uses a narrower definition. Since the broader Title I definition governs how U.S. person queries are conducted pursuant to the relevant minimization procedures, it will be used throughout this report.

- **Target.** Within the IC, the term “target” has multiple meanings. With respect to the statistics provided in this report, the term “target” is defined as the individual person, group, entity composed of multiple individuals, or foreign power that uses the selector such as a telephone number or email address.
- **Orders.** There are different types of orders that the FISC may issue in connection with FISA cases, for example: orders granting or modifying the government’s authority to conduct foreign intelligence collection; orders directing electronic communication service providers to provide any technical assistance necessary to implement the authorized foreign intelligence collection; and supplemental orders and briefing orders requiring the government to take a particular action or provide the court with specific information. The FISC may amend an order one or more times after it has been issued. For example, an order may be amended to add a newly discovered account used by the target. This report does not count such amendments separately. The FISC may renew some orders multiple times during the calendar year. Each authority permitted under FISA has specific time limits for the FISA authority to continue (e.g., a Section 704 order against a U.S. person target outside of the United States may last no longer than 90 days but FISA permits the order to be renewed, *see* 50 U.S.C. § 1881c(c)(4)). Each renewal requires a separate application submitted by the government to the FISC and a finding by the FISC that the application meets the requirements of FISA. Thus, unlike amendments, this report does count each such renewal as a separate order. These terms will be used consistently throughout this report.
- **“Estimated Number.”** Throughout this report, when numbers are *estimated*, the estimate comports with the statutory requirements to provide a “good faith estimate” of a particular number.
- **Dissemination.** In the most basic sense, dissemination refers to the sharing of minimized information. As it pertains to FISA (including Section 702), if an agency (in this instance NSA) lawfully collects information pursuant to FISA and wants to disseminate that information, the agency must first apply its minimization procedures to that information.

FISA Probable Cause Authorities

A. FISA Titles I and III

To conduct electronic surveillance or physical search under FISA Title I or FISA Title III, a probable cause court order is required regardless of U.S. person status.

Under FISA, Title I permits electronic surveillance and Title III permits physical search in the United States of foreign powers or agents of a foreign power for the purpose of collecting foreign intelligence information. See 50 U.S.C. §§ 1804 and 1823. Title I (electronic surveillance) and Title III (physical search)

are commonly referred to as “Traditional FISA.” Both require that the FISC make a probable cause finding, based upon a factual statement in the government’s application, that (i) the target is a foreign power or an agent of a foreign power, as defined by FISA and (ii) the facility being targeted for electronic surveillance is used by or about to be used, or the premises or property to be searched is or is about to be owned, used, possessed by, or is in transit to or from a foreign power or an agent of a foreign power. In addition to meeting the probable cause standard, the government’s application must meet the other requirements of FISA. See 50 U.S.C. §§ 1804(a) and 1823(a).

FISA Title I, Title III, and Title VII Section 703 and 704

→ All of these authorities require individual court orders based on probable cause.

→ Titles I and III apply to FISA activities directed against persons within the United States.

→ Sections 703 and 704 apply to FISA activities directed against U.S. persons outside the United States.

B. FISA Title VII, Sections 703 and 704

FISA Title VII Sections 703 and 704 similarly require a court order based on a finding of probable cause for the government to undertake FISA activities targeting U.S. persons located outside the United States. Section 703 applies when the government seeks to conduct electronic surveillance or to acquire stored electronic communications or stored electronic data, in a manner that otherwise requires an order pursuant to FISA, of a U.S. person who is reasonably believed to be located outside the United States. Section 704 applies when the government seeks to conduct collection overseas targeting a U.S. person reasonably believed to be located outside the United States under circumstances in which the U.S. person has a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted in the United States. Both Sections 703 and 704 require that the FISC make a

probable cause finding, based upon a factual statement in the government’s application, that the target is a U.S. person reasonably believed to be (i) located outside the United States and (ii) a foreign power, agent of a foreign power, or officer or employee of a foreign power. Additionally, the government’s application must meet the other requirements of FISA. See 50 U.S.C. §§ 1881b(b) and 1881c(b).

C. Statistics

How targets are counted. If the IC received authorization to conduct electronic surveillance and/or physical search against the same target in four separate applications, the IC would count one target, not four. Alternatively, if the IC received authorization to conduct electronic surveillance and/or physical search against four targets in the same application, the IC would count four targets. Duplicate targets across authorities are not counted.

Figure 1a: Table of FISA “Probable Cause” Court Orders and Targets

<u>Titles I and III and Sections 703 and 704 of FISA</u>	CY2013	CY2014	CY2015	CY2016	CY2017
Total number of orders	1,767	1,519	1,585	1,559	1,437
Estimated number of targets of such orders*	1,144	1,562	1,695	1,687	1,337

See 50 U.S.C. §§ 1873(b)(1) and 1873(b)(1)(A).

* Although providing this statistic was first required by the USA FREEDOM Act, the reauthorized FAA of 2017 enumerated this requirement at 50 U.S.C. § 1873(b)(1)(A).

Figure 1b: Chart of FISA “Probable Cause” Court Orders and Targets

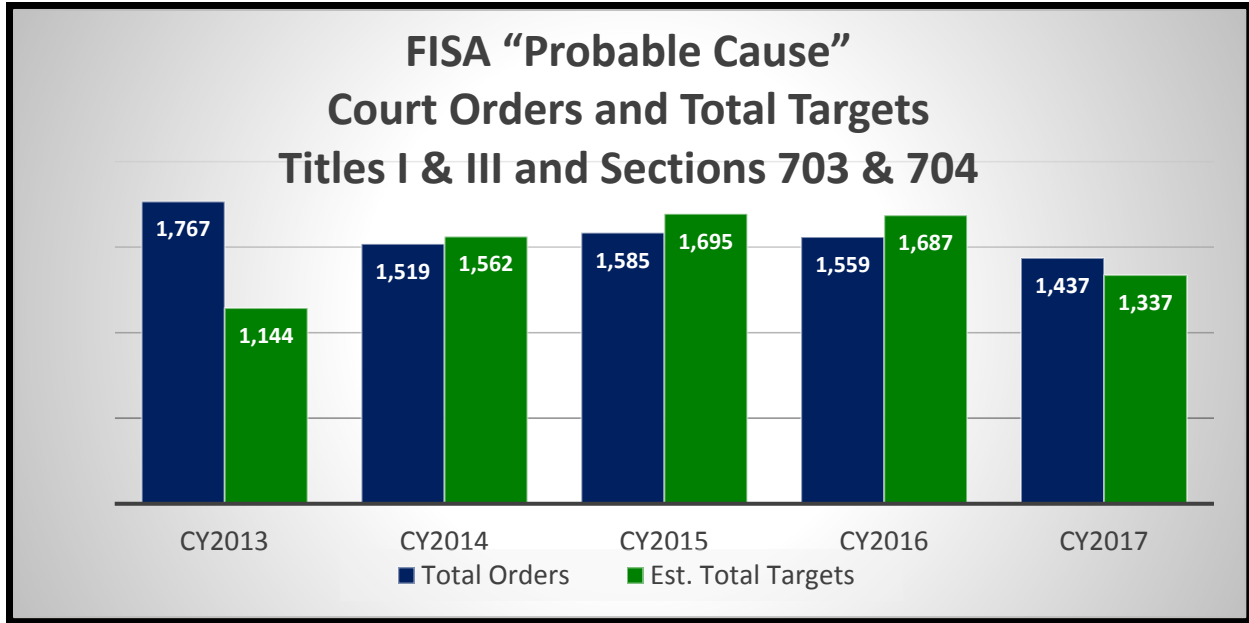


Figure 2: Table of FISA “Probable Cause” Targets – U.S. Persons

<u>Titles I and III and Sections 703 and 704 -- Targets</u>	CY2016	CY2017
Estimated number of targets who are <i>non</i> -U.S. persons*	1,351	1,038
Estimated number of targets who are U.S. persons*	336	299
Estimated percentage of targets who are U.S. persons	19.9%	22.4%

See 50 U.S.C. §§1873(b)(1)(B) and 1873(b)(1)(C) for rows one and two, respectively.

* Previously the IC was not statutorily required to publicly provide these statistics but provided them consistent with transparency principles. The reauthorized FAA of 2017 codified this requirement at 50 U.S.C. §§ 1873(b)(1)(B) and 1873(b)(1)(C).

FISA Section 702

A. Section 702

Title VII of FISA includes Section 702, which permits the Attorney General and the DNI to jointly authorize the targeting of (i) non-U.S. persons (ii) reasonably believed to be located outside the United States (iii) to acquire foreign intelligence information. See 50 U.S.C. § 1881a. All three elements must be met.

Additionally, Section 702 requires that the Attorney General, in consultation with the DNI, adopt targeting procedures, minimization procedures, and querying procedures that they attest satisfy the statutory requirements and are consistent with the Fourth Amendment. Additional information on how the government uses Section 702 is posted on *IC on the Record*.

Section 702 Targets and “Tasking.” Under Section 702, the government “targets” a particular non-U.S. person, group, or entity reasonably believed to be located outside the United States and who possesses, or who is likely to communicate or receive, foreign intelligence information, by directing an acquisition at – i.e., “tasking” – selectors (e.g., telephone numbers and email addresses) that are assessed to be used by such non-U.S. person, group, or entity, pursuant to targeting procedures approved by the FISC. Before “tasking” a selector for collection under Section 702, the government must apply its targeting procedures to ensure that the IC appropriately tasks a selector used by a non-U.S. person who is reasonably believed to be located outside the United States and who will likely possess, communicate, or receive foreign intelligence information.

NSA and FBI task selectors pursuant to their respective Section 702 targeting procedures, which are discussed below. All agencies that receive unminimized (i.e., “raw”) Section 702 data – NSA, FBI, Central Intelligence Agency (CIA), and National Counterterrorism Center (NCTC) – handle the Section 702-acquired data in accordance with minimization procedures, which are explained below.

Title VII - FISA Amendments Act (FAA) Section 702

→ Commonly referred to as “Section 702.”

→ Requires individual targeting determinations that the target (1) is a non-U.S. person (2) who is reasonably believed to be located outside the United States and (3) who has or is expected to communicate or receive foreign intelligence information.

The FISC's role. Under Section 702, the FISC determines whether *certifications* provided jointly by the Attorney General and the DNI meet all the requirements of Section 702. If the FISC determines that the government's certifications its targeting, minimization, and, as described below, querying procedures meet the statutory requirements of Section 702 and are consistent with the Fourth Amendment, then the FISC issues an order and supporting statement approving the certifications. The [2016 FISC order and statement approving certifications](#) was publicly released in May 2017 and posted on *IC on the Record*.

Certifications. The certifications are jointly executed by the Attorney General and DNI and authorize the government to acquire foreign intelligence information under Section 702. Each annual certification application package must be submitted to the FISC for approval. The package includes the Attorney General and DNI's certifications, affidavits by certain heads of intelligence agencies, targeting procedures, minimization procedures, and, as described below, querying procedures. [Samples of certification application packages](#) have been publicly released on *IC on the Record*, most recently in [May 2017](#). The certifications identify categories of information to be collected, which must meet the statutory definition of foreign intelligence information, through the targeting of non-U.S. persons reasonably believed to be located outside the United States. The certifications have included information concerning international terrorism and other topics, such as the acquisition of information concerning weapons of mass destruction.

Targeting procedures. The targeting procedures detail the steps that the government must take before tasking a selector, as well as verification steps after tasking, to ensure that the user of the tasked selector is being targeted appropriately – specifically, that the user is a non-U.S. person, located outside the United States, who is being tasked to acquire foreign intelligence information. The IC must make individual determinations that each tasked selector meets the requirements of the targeting procedures. Each agency's Section 702 targeting procedures are approved by the Attorney General and then reviewed, as part of the certification package, by the FISC, which reviews the sufficiency of each agency's targeting procedures including assessing the IC's compliance with the procedures. [NSA's targeting procedures \(signed in 2017\) for the 2016 certification package](#) have been publicly released *IC on the Record*.

Minimization procedures. The minimization procedures detail requirements the government must meet to use, retain, and disseminate Section 702 data, which include specific restrictions on how the IC handles non-publicly available U.S. person information acquired from Section 702 collection of non-U.S. person targets, consistent with the needs of the government to obtain, produce, and disseminate foreign intelligence information. Each agency's Section 702 minimization procedures are approved by the Attorney General and then reviewed, as part of the certification package, by the FISC, which reviews the sufficiency of each agency's

minimization procedures, including assessing the IC's compliance with past procedures. The [2016 certification minimization procedures](#) have been released on *IC on the Record*.

Querying procedures. With the reauthorized FAA of 2017, Congress amended Section 702 to require that querying procedures be adopted by the Attorney General, in consultation with the DNI. Section 702(f) requires that a record of each U.S. person query term be kept. Similar to the other procedures, the querying procedures are required to be reviewed by the FISC as part of the certification package for consistency with the statute and the Fourth Amendment. Congress added other requirements in 702(f), which pertain to the access of certain results of queries conducted by FBI; those requirements will be discussed later in this report.

To date, each agency's court-approved minimization procedures have provided the rules under which the agency may query their databases containing previously acquired Section 702 data (content and metadata) using a U.S. person query term. As described above, with the reauthorized FAA of 2017, Congress amended Section 702 to require that, going forward, querying procedures must be adopted by the Attorney General. Query terms may be date-bound, and may include alphanumeric strings, such as telephone numbers, email addresses, or terms, such as a name, that can be used individually or in combination with one another. Pursuant to court-approved procedures, an agency can only query Section 702 information if the query is reasonably likely to return foreign intelligence information or, in the case of the FBI, evidence of a crime. Additional information about U.S. person queries is posted on *IC on the Record*.

Compliance. The IC's adherence to the targeting and minimization procedures, including query requirements, is subject to [robust internal agency oversight and to rigorous external oversight by the Department of Justice \(DOJ\), ODNI, Congress, and the FISC](#). Every identified incidence of non-compliance is reported to the FISC (through individual notices or in reports) and to Congress in semiannual reports. DOJ and ODNI also submit semiannual reports to Congress that assess the IC's overall compliance efforts. [Past assessments](#) have been publicly released.

B. Statistics—Orders and Targets

Counting Section 702 orders. As explained above, the FISC may issue a single order to approve more than one Section 702 certification to acquire foreign intelligence information. Note that, in its own transparency report, which is required pursuant to 50 U.S.C. § 1873(a), the Director of the Administrative Office of the United States Courts (AOUSC) counted each of the Section 702 certifications associated with the FISC's order. Because the number of the government's Section 702 certifications remains a classified fact, the government requested that the AOUSC redact the number of certifications from its transparency report prior to publicly releasing it.

[In 2016](#), the government submitted a certification application package to the FISC. Pursuant to 50 U.S.C. § 1881a(j)(2), [the FISC extended its review of the 2016 certification package](#). The FISC may extend its review of the certifications “as necessary for good cause in a manner consistent with national security.” See 50 U.S.C. § 1881a(j)(2) (note that with the reauthorized FAA of 2017, this section has been updated to § 1881a(k)(2)). Thus, because the FISC did not complete its review of the 2016 certifications during calendar year 2016, the FISC did not issue an order concerning those certifications in calendar year 2016. The 2015 order remained in effect during the extension period. On April 26, 2017, the [FISC issued an order authorizing the 2016 certifications](#).

Figure 3: Table of Section 702 Orders

<u>Section 702 of FISA</u>	CY2013	CY2014	CY2015	CY2016	CY2017
Total number of orders issued	1	1	1	0	1

See 50 U.S.C. § 1873(b)(2).

Estimating Section 702 targets. The number of 702 “targets,” provided below, reflects an estimate of the number of non-U.S. persons who are the users of tasked selectors. This estimate is based on information readily available to the IC. Unless and until the IC has information that links multiple selectors to a single foreign intelligence target, each individual selector is counted as a separate target for purposes of this report. On the other hand, where the IC is aware that multiple selectors are used by the same target, the IC counts the user of those selectors as a single target. This counting methodology reduces the risk that the IC might inadvertently understate the number of discrete persons targeted pursuant to Section 702.

Figure 4: Table of Section 702 Targets (recall that only non-USPs are targeted)

<u>Section 702 of FISA</u>	CY2013	CY2014	CY2015	CY2016	CY2017
Estimated number of targets of such orders*	89,138	92,707	94,368	106,469	129,080

See 50 U.S.C. § 1873(b)(2)(A).

* Previously the IC was not statutorily required to publicly provide this statistic, but provided it consistent with transparency principles. The reauthorized FAA of 2017 codified this requirement at 50 U.S.C. § 1873(b)(2)(A).

C. Statistics—U.S. Person Queries

In July 2014, the Privacy and Civil Liberties Oversight Board (PCLOB or Board) issued a report on Section 702 entitled, “*Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*” (PCLOB’s Section 702 Report), which reported U.S. person query statistics for calendar year 2013. See PCLOB’s Section 702 Report, at 57-58. The USA FREEDOM Act, enacted in 2015, required the public reporting of statistics regarding the number of U.S. person queries of Section 702. Specifically, the Act required the “number of search terms concerning a known United States person used to retrieve the unminimized contents [...]” – referred as *query terms of content* – and “the number of queries concerning a known United States person of unminimized noncontents information [...]” – referred as *queries of metadata*. See 50 U.S.C. § 1873(b)(2)(B) and (b)(2)(C), respectively. Thus, ODNI began reporting on these statistics in the *Annual Statistical Transparency Report* covering calendar year 2015.

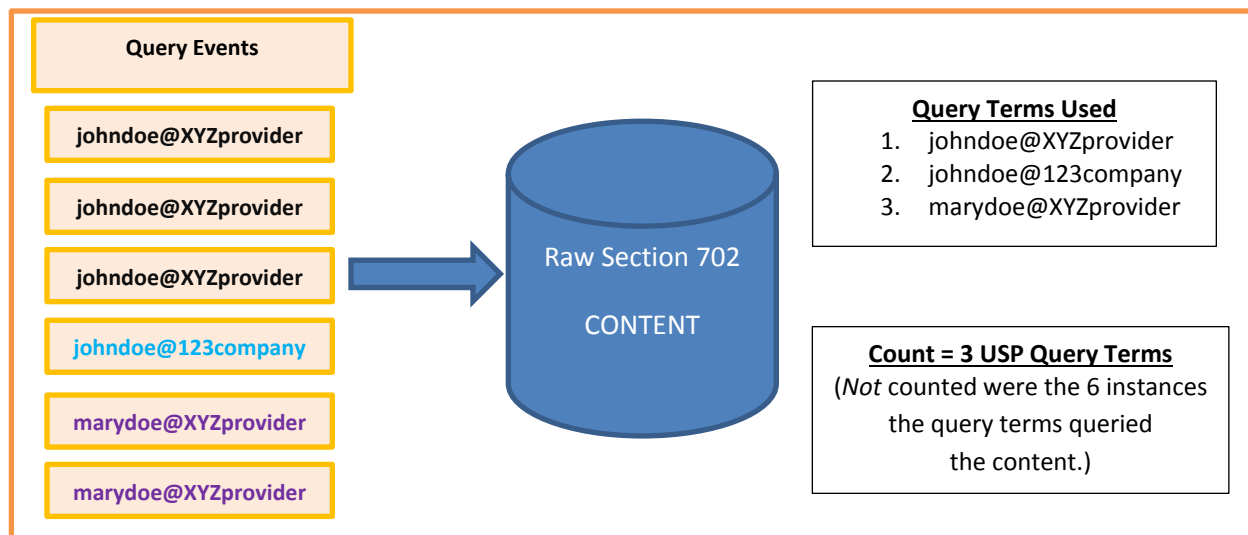
Below are statistics for U.S. person queries of raw, unminimized Section 702-acquired data.¹ The U.S. person statistics are based on (a) approved U.S. person *query terms* used to query

¹ With the reauthorization of FAA in 2017, Congress codified new requirements regarding the access of results of certain queries conducted by the FBI. Specifically under Section 702(f)(2)(A), an order from the FISC is now required before the FBI can review the contents of a query using a U.S. person query term when the query was not designed to find and extract foreign intelligence information and was performed in connection with a predicated criminal investigation that does not relate to national security. Before the FISC may issue such an order based on a finding of probable cause, an FBI officer must apply in writing, to include the officer’s justification that the query results would provide evidence of criminal activity, and the application must be approved by the Attorney General.

Section 702 *content* and (b) U.S. person *queries* conducted of Section 702 *noncontents* (i.e., metadata). It is important to understand that these two very different numbers cannot be combined because they use *different counting methodologies* (approved query terms versus queries conducted) and *different data types* (content versus noncontents).

Counting approved U.S. person query terms used to query Section 702 content. The NSA counts the number of U.S. person identifiers it approved to query the content of unminimized Section 702-acquired information. For example, if the NSA used U.S. person identifier “johndoe@XYZprovider” to query the content of Section 702-acquired information, the NSA would count it as one regardless of how many times the NSA used “johndoe@XYZprovider” to query its 702-acquired information. The CIA started using this model in 2016 for counting query terms and those statistics were included in the *Annual Statistical Transparency Report* covering CY2016. When the NCTC began receiving raw Section 702 information, NCTC followed a similar approach of counting U.S. person query terms that were used to query Section 702 content.

Figure 5: Illustration of how the IC counts approved U.S. person query terms used to query Section 702 content



50 U.S.C. Section 1873(b)(2)(A) requires annual reporting of the number of times the FBI received an order pursuant to 702(f)(2)(A); this statistic will be provided in future transparency reports.

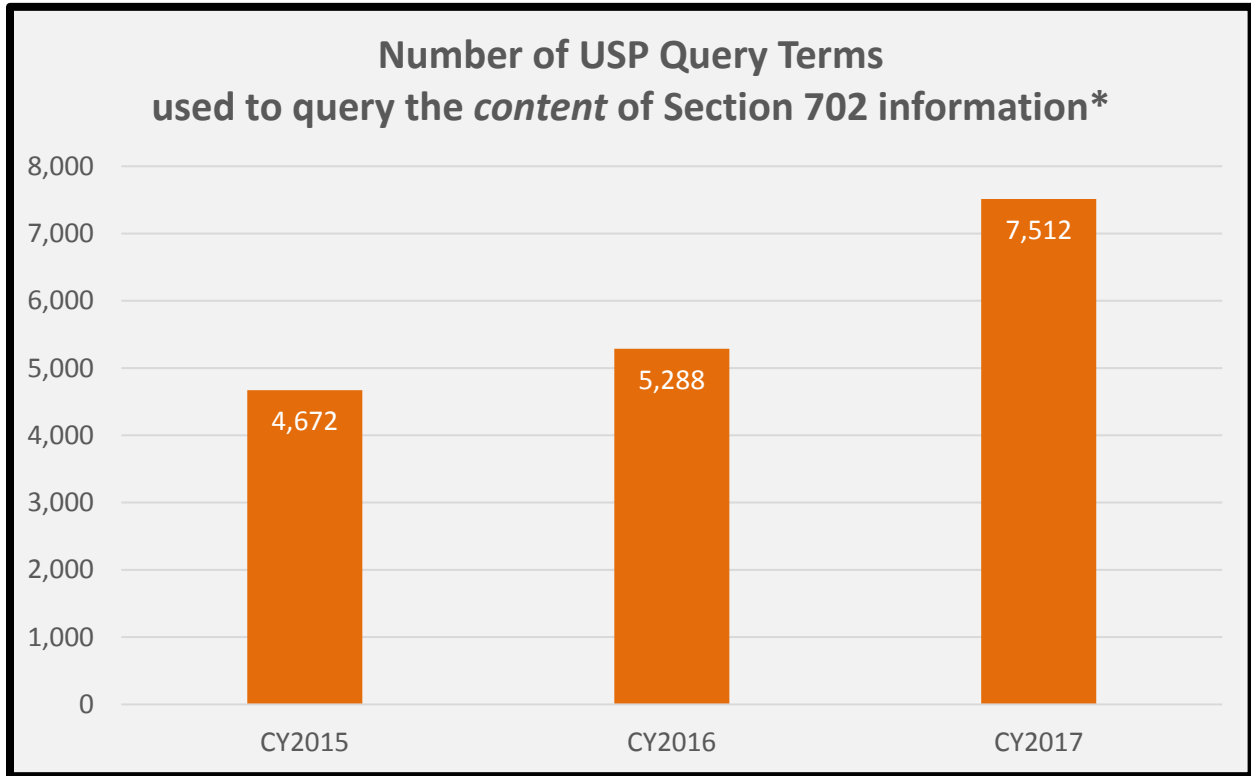
Figure 6a: Table of U.S. Person Query Terms Used to Query Section 702 Content

<u>Section 702 of FISA</u>	CY2015	CY2016	CY2017
Estimated number of search terms concerning a known U.S. person used to retrieve the unminimized contents of communications obtained under Section 702 (excluding search terms used to prevent the return of U.S. person information)*	4,672	5,288	7,512

See 50 U.S.C. § 1873(b)(2)(B).

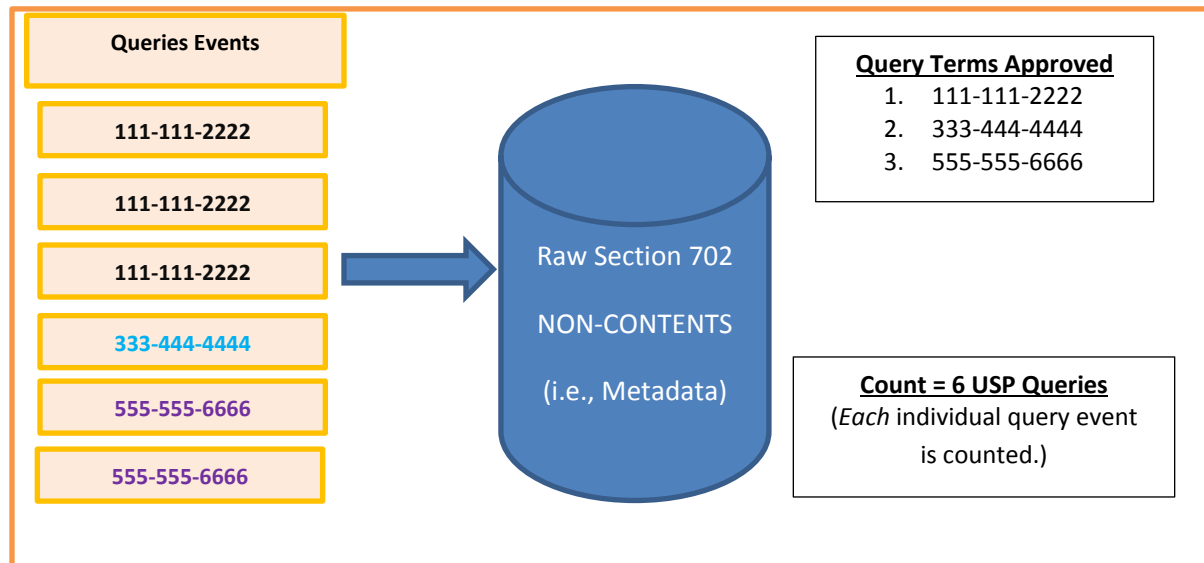
* Consistent with 50 U.S.C. § 1873(d)(2)(A), this statistic does not include queries that are conducted by the FBI. However, the reauthorized FAA of 2017 codified a new reporting requirement for the FBI under 50 U.S.C. § 1873(b)(2)(D), which is addressed later in this report.

Figure 6b: Chart of U.S. Person Query Terms Used to Query Section 702 Content



Counting queries using U.S. person identifiers of noncontents collected under Section 702.

This estimate represents the number of times a U.S. person identifier is used to query the noncontents (i.e., metadata) of unminimized Section 702-acquired information. For example, if the U.S. person identifier telephone number “111-111-2222” was used 15 times to query the noncontents of Section 702-acquired information, the number of queries counted would be 15.

Figure 7: Illustration of how the IC counts U.S. person queries of Section 702 noncontents

As with last year’s transparency report, one IC element, the CIA, remains currently unable to provide the number of queries using U.S. person identifiers of unminimized Section 702 noncontents information for CY2017. Under 50 U.S.C. § 1873(d)(3)(A), if the DNI concludes that this good-faith estimate cannot be determined accurately because not all of the relevant elements of the IC are able to provide this good faith estimate, then the DNI is required to (i) certify that conclusion in writing to the relevant Congressional committees; (ii) report the good faith estimate for those relevant elements able to provide such good faith estimate; (iii) explain when it is reasonably anticipated that such an estimate will be able to be determined fully and accurately; and (iv) make such certification publicly available on an Internet web site. Because the CIA remained unable to provide such information for calendar year 2017, the DNI made a certification, pursuant to 50 U.S.C. § 1873(d)(3)(A) to the relevant Congressional committees. As required by statute, this certification is being made publicly available as an attached appendix to this current report (see Appendix A). As described in Appendix A, CIA will be able to provide a good faith estimate of these queries for calendar year 2018; such information will be included in the 2019 annual transparency report.

Figure 8: Table of U.S. Person Queries of Noncontents of Section 702

<u>Section 702 of FISA</u>	CY2013	CY2014	CY2015	CY2016	CY2017
Estimated number of queries concerning a known U.S. person of unminimized noncontents information obtained under Section 702 (excluding queries containing information used to prevent the return of U.S. person information)*	9,500	17,500	23,800	30,355	16,924

See 50 U.S.C. § 1873(b)(2)(C).

* Consistent with 50 U.S.C. § 1873(d)(2)(A), this statistic does not include queries that are conducted by the FBI. However, the reauthorized FAA of 2017 codified a new reporting requirement for the FBI under 50 U.S.C. § 1873(b)(2)(D), which was addressed earlier in this report.

FISC Order Requiring Certain Section 702 Query Reporting by FBI. On November 6, 2015, the FISC granted the government’s application for renewal of the 2015 certifications and, among other things, concluded that the FBI’s U.S. person querying provisions in its minimization procedures, “strike a reasonable balance between the privacy interests of the United States persons and persons in the United States, on the one hand, and the government’s national security interests, on the other.” [Memorandum Opinion and Order dated November 6, 2015](#), at 44 (released on *IC on the Record* on April 19, 2016). The FISC further stated that the FBI conducting queries, “designed to return evidence of crimes unrelated to foreign intelligence does not preclude the Court from concluding that taken together, the targeting and minimization procedures submitted with the 2015 Certifications are consistent with the requirements of the Fourth Amendment.” *Id.*

Nevertheless, the FISC ordered the government to report in writing, “each instance after December 4, 2015, in which FBI personnel *receive and review* Section 702-acquired information that the FBI identifies as concerning a United States person in response to a query that is not designed to find and extract foreign intelligence information.” (Emphasis added). *Id.* at 44 and 78. The FISC directed that the report contain details of the query terms, the basis for conducting the query, the manner in which the query will be or has been used, and other details. *Id.* at 78. In keeping with the IC’s *Principles of Transparency*, the DNI declassified the number of each such query reported to the FISC in calendar year 2016. This year, the DNI has again declassified the number reported for calendar year 2017, as noted in Figure 10.

Figure 9: Table Regarding Required Section 702 Query Reporting to the FISC

<u>Section 702 of FISA</u>	CY2016	CY2017
Per the FISC Memorandum Opinion and Order dated November 6, 2015: Each reported instance in which FBI personnel <i>received and reviewed</i> Section 702-acquired information that the FBI identified as concerning a U.S. person in response to a query that was designed to return evidence of a crime unrelated to foreign intelligence.	1	0

D. Section 702 and FBI Investigations.

The reauthorized FAA of 2017 now requires that the FBI report on the number of instances in which the FBI opened a criminal investigation of a U.S. person, who is not considered a threat to national security, based wholly or in part on Section 702-acquired information. See 50 U.S.C. § 1873(b)(2)(D). This statistic will provide transparency with regard to how often Section 702 collection is used for non-national security investigations conducted by the FBI. Figure 10 provides the required statistic.

Figure 10: Table Regarding Number of FBI Investigations Opened on USPs Based on Section 702 Acquisition

<u>Section 702 of FISA</u>	CY2017
The number of instances in which the FBI opened, under the Criminal Investigative Division or any successor division, an investigation of a U.S. person (who is not considered a threat to national security) based wholly or in part on an acquisition authorized under Section 702.	0

See 50 U.S.C. § 1873(b)(2)(D).

NSA Dissemination of U.S. Person Information under FISA Section 702

A. Section 702

In July 2014, the PCLOB's *Section 702 Report* contained 10 recommendations. Recommendation 9 focused on "accountability and transparency," noting that the government should implement measures, "to provide insight about the extent to which the NSA acquires and utilizes the communications involving U.S. persons and people located in the United States under the Section 702 program." *PCLOB's Section 702 Report* at 145-146. Specifically, the PCLOB recommended that "the NSA should implement processes to annually count [...] (5) the number of instances in which the NSA disseminates non-public information about U.S. persons, specifically distinguishing disseminations that includes names, titles, or other identifiers, such as telephone numbers or e-mail addresses, potentially associated with individuals." *Id.* at 146. This recommendation is commonly referred to as Recommendation 9(5). In response to the PCLOB's July 2014 Recommendation 9(5), NSA previously publicly provided (in the *Annual Statistical Transparency Report* for calendar year 2015) and continues to provide the following additional information regarding the dissemination of Section 702 intelligence reports that contain U.S. person information. Because the PCLOB issued its recommendation in 2014, these statistics were not included in *Annual Statistical Transparency Report* for calendar years 2013 or 2014.

NSA has been providing similar information to Congress since 2009, in classified form, per FISA reporting requirements. For example, FISA Section 702(m)(3) requires that NSA annually submit a report to applicable Congressional committees regarding certain numbers pertaining to the acquisition of Section 702-acquired information, including the number of "disseminated intelligence reports containing a reference to a United States person identity." See 50 U.S.C. § 1881a(m)(A)(3)(i) (prior to the reauthorized FAA of 2017 under § 1881a(l)(3)(A)(i)). Section 702a(m)(A)(3) also requires that the number of "United States-person identities subsequently disseminated by [NSA] in response to request for identities that were not referred to by name or title in the original reporting." See 50 U.S.C. § 1881a(m)(3)(A)(ii). This second requirement refers to NSA providing the number of approved unmasking requests, which is explained below. Additionally, NSA provides the number of NSA's disseminated intelligence reports containing a U.S. person reference to Congress as part of the Attorney General and the DNI's joint assessment of compliance. See 50 U.S.C. § 1881a(m)(1) (prior to the reauthorized FAA of 2017 under § 1881a(l)(1)).

Prior to the PCLOB issuing its *Section 702 Report*, NSA's Director of the Civil Liberties, Privacy, and Transparency Office published "*NSA's Implementation of Foreign Intelligence Surveillance Act Section 702*," on April 16, 2014, (hereinafter "[NSA DCLPO Report](#)"), in which it explained

NSA's dissemination processes. *NSA DCLPO Report* at 7-8. NSA "only generates classified intelligence reports when the information meets a specific intelligence requirement, regardless of whether the proposed report contains U.S. person information." *NSA DCLPO Report* at 7.

Section 702 only permits the targeting of non-U.S. persons reasonably believed to be located outside the United States to acquire foreign intelligence information. Such targets, however, may communicate information to, from, or about U.S. persons. [NSA minimization procedures](#) (publicly released on May 11, 2017) permit the NSA to disseminate U.S. person information if the NSA masks the information that could identify the U.S. person. The minimization procedures also permit NSA to disseminate the U.S. person identity only if doing so meets one of the specified reasons listed in NSA's minimization procedures, including that the U.S. person consented to the dissemination, the U.S. person information was already publicly available, the U.S. person identity was necessary to understand foreign intelligence information, or the communication contained evidence of a crime and is being disseminated to law enforcement authorities. Even if one these conditions applies, as a matter of policy, NSA may still mask the U.S. person information and will include no more than the minimum amount of U.S. person information necessary to understand the foreign intelligence or to describe the crime or threat. *Id.* In certain instances, however, NSA makes a determination prior to releasing its original classified report that the U.S. person's identity is appropriate to disseminate in the first instance using the same standards discussed above.

Masked U.S. Person Information. Agency minimization procedures generally provide for the substitution of a U.S. person identity with a generic phrase or term if the identity otherwise does not meet the dissemination criteria; this is informally referred to as "masking" the identity of the U.S. person. Information about a U.S. person is masked when the identifying information about the person is not included in a report. For example, instead of reporting that Section 702-acquired information revealed that non-U.S. person "Bad Guy" communicated with U.S. person "John Doe" (i.e., the actual name of the U.S. person), the report would mask "John Doe's" identity, and would state that "Bad Guy" communicated with "an identified U.S. person," "a named U.S. person," or "a U.S. person."

Unmasking U.S. Person Information. Recipients of NSA's classified reports, such as other federal agencies, may request that NSA provide the U.S. person identity that was masked in an intelligence report. The requested identity information is released only if the requesting recipient has a "need to know" the identity of the U.S. person and if the dissemination of the U.S. person's identity would be consistent with NSA's minimization procedures (e.g., the identity is necessary to understand foreign intelligence information or assess its importance), and additional approval has been provided by a designated NSA official.

As part of their regular oversight reviews, DOJ and ODNI review disseminations of information about U.S. persons that NSA obtained pursuant to Section 702 to ensure that the disseminations were performed in compliance with the minimization procedures.

Additional information describing how the IC protects U.S. person information obtained pursuant to FISA provisions is provided [in recent reports by the civil liberties and privacy officers for the ODNI](#) (including NCTC), NSA, FBI, and CIA. The reports collectively documented the rigorous and multi-layered framework that safeguards the privacy of U.S. person information in FISA disseminations. See [ODNI Report on Protecting U.S. Person Identities in Disseminations under FISA](#) and [annexes containing agency specific reports](#).

B. Statistics

Below are statistics and charts to further explain how NSA disseminates U.S. person information incidentally acquired from Section 702 in classified intelligence reports. NSA may:

- i. openly name (i.e., originally reveal) the U.S. person in the report,
- ii. initially mask (i.e., not reveal) the U.S. person identity in the report, or
- iii. in the instances where the U.S. person identity was initially masked, upon a specific request, later reveal and unmask the U.S. person identity but only to the requestor.

This year's report presents the dissemination numbers in a different format from the previous report to facilitate understanding and to provide consistency with NSA's classified FISA Section 702(m)(3) reports to Congress. This report separates the number of reports (in Figure 11) from the statistics relating to the U.S. person identities later disseminated (in Figure 12).

NSA applies its minimization procedures in preparing its classified intelligence reports, and then disseminates the reports to authorized recipients with a need to know the information in order to perform their official duties. Very few of NSA's intelligence reports from Section 702 collection contain references to U.S. person identities (whether masked or openly named).

The first row of Figure 11 provides "an accounting of the number of disseminated intelligence reports containing a reference to a United States-person identity." See 50 U.S.C. § 1881a(m)(3)(A)(i). Note that a single report could contain multiple U.S. person identities, masked and/or openly named. NSA's counting methodology is to include any disseminated intelligence report that contains a reference to one or more U.S. person identities, whether masked or openly named, even if the report includes information from other sources. NSA does not maintain records that allow it to readily determine, in the case of an intelligence report that includes information from several sources, from which source a reference to a U.S. person identity was derived. Accordingly, the references to U.S. person identities may have resulted

from Section 702 authorized collection or from other authorized signals intelligence activity conducted by NSA. This counting methodology was used in the previous report and is used in NSA's FISA Section 702(m)(3) report. As noted above, a U.S. person is "a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in [50 U.S.C. § 1801(a)(1), (2), or (3)]." See 50 U.S.C. § 1801(i).

The second row of Figure 11 provides the *number of reports* containing U.S. person identities where the U.S. person identity was masked in the report. The third row provides the *number of reports* containing U.S. person identities where the U.S. person was openly named in the report.

Figure 11: Table of Section 702 Reports Containing USP information unmasked by NSA

<u>Section 702 Reports Containing U.S. person (USP) information disseminated by NSA</u>	CY2016	CY2017
Reports – Total number of NSA disseminated §702 reports containing USP identities <i>regardless of whether the identity was openly named or masked.</i>	3,914	4,065
Reports – Total number of NSA disseminated §702 reports containing USP identities <i>where the USP identity was masked.</i>	2,964	3,034
Reports – Total number of NSA disseminated §702 reports containing USP identities <i>where the USP was openly named.</i>	1,200	1,341

As explained above, rows 2 and 3 will not total row 1 because one report may contain both masked and openly named identities.

Figure 12 provides statistics relating to the numbers of U.S. person identities that were originally masked in those reports counted in Figure 11 but which NSA later provided to authorized requestors (i.e., unmasked) during CY2017. This statistic is the number required to be reported to Congress in NSA's FISA Section 702(m)(3) report. In other words, Figure 12 provides "an accounting of the number of United States-person identities subsequently disseminated by [NSA] in response to requests for identities that were not referred to by name or title in the original reporting." See 50 U.S.C. § 1881a(m)(3)(A)(ii). This number is different than numbers provided in either CY2015 or the CY2016 *Annual Statistical Transparency Report*. NSA has decided to declassify the total number of U.S. person identities unmasked in response to a request. The U.S. person identities include individuals as well as non-individual entities

whose identities NSA masks pursuant to law or policy. These non-individual entities, include, for example, U.S. IP addresses and artificial “persons” such as corporations.

Previously, the *Annual Statistical Transparency Report* focused on responding to the PCLOB’s report recommendation 9(5) by counting only those U.S. person identities where the proper name or title of an individual was unmasked; it did not count any other unmasking such as email addresses or telephone numbers or U.S. IP addresses or U.S. corporations. Rather than distinguishing between the different ways a U.S. person might be named in an intelligence report, NSA will provide the total number of U.S. person identities unmasked in response to a specific request from another agency whether it is a title of an individual, an identifier such as an email address, an IP address or a corporation. Thus, this current *Annual Statistical Transparency Report*, in Figure 12, reports that same metric that is reported in NSA’s FISA Section 702(m)(3). However, because NSA’s FISA Section 702(m)(3) reports have a time period of September through August, comparing the two reporting years is not an exact comparison.

Figure 12: Table of Section 702 USP Identities disseminated by NSA

<u>Section 702 – U.S. person (USP) identities unmasked by NSA</u>	12 month period Sep 2015-Aug 2016	CY2017
The number of U.S. person identities that NSA unmasked in response to a specific request from another agency.	9,217	9,529

Beginning with next year’s transparency report (due April 2019), ODNI will report statistics pertaining to how the IC disseminates U.S. person information regardless of the legal authority under which the information was collected (not only FISA Section 702). See [ICPG 107.1](#). Specifically, ODNI will report (1) the total number of requests to identify U.S. persons, whose identity was originally omitted, in disseminated intelligence reports, (2) the total number of those requests approved, and (3) the total number of those requests denied.

FISA Criminal Use and Notice Provisions

A. FISA Sections 106 and 305

FISA Section 106 requires advance authorization from the Attorney General before any information acquired through Title I electronic surveillance may be used in a criminal proceeding. This authorization from the Attorney General is defined to include authorization by the Acting Attorney General, Deputy Attorney General, or, upon designation by the Attorney General, the Assistant Attorney General for National Security. Section 106 also requires that if a government entity intends to introduce into evidence in any trial, hearing, or other proceeding, against an aggrieved person, information obtained or derived from electronic surveillance, it must notify the aggrieved person and the court. The aggrieved person is then entitled to seek suppression of the information. FISA Section 706 requires that any information acquired pursuant to Section 702 be treated as electronic surveillance under Title I, including for purposes of the use, notice, and suppression requirements under Section 106.

FISA Section 305 provides the same requirements for information acquired through Title III physical search (i.e., advance authorization, notice, and opportunity to suppress).

B. Statistics

The reauthorized FAA of 2017 codified that certain statistics concerning criminal proceedings must be provided to the public pertaining to Sections 106 and 305, including Section 702-acquired information. Specifically, figure 13 provides that, in 2017, the Government filed notice of intent to use FISA-acquired information, pursuant to Section 106 or 305, in seven (7) separate criminal proceedings.

FISA Sections 106 and 305 – Criminal Use and Notice Provisions –

→ Commonly referred to as the “criminal use provision.”

→ Section 106 applies to information acquired from Title I electronic surveillance; Section 305 applies to information acquired from Title III physical search.

→ Attorney General advance authorization is required before such information may be used in a criminal proceeding; if such information is used or intended to be used against an aggrieved person, that person must be given notice of the information and have a chance to suppress the information.

→ The reauthorized FAA of 2017 codified that statistics must be provided to the public as it pertained to Section 106, Section 305, as well as Section 702 acquired information.

Figure 13: Table Regarding Number of Criminal Proceedings in which the Government Provided Notice of Its Intent to Use Cert FISA Information

<u>FISA Sections 106 and 305</u>	CY2017
<p>The number of criminal proceedings in which the United States or a State or political subdivision thereof provided notice pursuant to Section 106 (including with respect to Section 702-acquired information) or Section 305 of the government’s intent to enter into evidence or otherwise use or disclose any information obtained or derived from electronic surveillance, physical search, or Section 702 acquisition.</p>	<p>7</p>

FISA Title IV – Use of Pen Register and Trap and Trace (PR/TT) Devices

A. FISA PR/TT Authority

Title IV of FISA authorizes the use of pen register and trap and trace (PR/TT) devices for foreign intelligence purposes. Title IV authorizes the government to use a PR/TT device to seek and capture dialing, routing, addressing or signaling (DRAS) information. The government may submit an application to the FISC for an order approving the use of a PR/TT device (i.e., PR/TT order) for (i) “any investigation to obtain foreign intelligence information not concerning a United States person or” (ii) “to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution.” 50 U.S.C. § 1842(a). If the FISC finds that the government’s application sufficiently meets the requirements of FISA, the FISC must issue an order for the installation and use of a PR/TT device.

FISA Title IV

→ Commonly referred to as the “PR/TT” provision.

→ Bulk collection is prohibited.

→ Requires individual FISC order to use PR/TT device to capture dialing, routing, addressing, or signaling (DRAS) information.

→ Government request to use a PR/TT device on U.S. person target must be based on an investigation to protect against terrorism or clandestine intelligence activities and that investigation must not be based solely on the basis of activities protected by the First Amendment to the Constitution.

B. Statistics

Counting orders. Similar to how orders were counted for Titles I and III and Sections 703 and 704, this report only counts the orders *granting authority to conduct intelligence collection* -- the order for the installation and use of a PR/TT device. Thus, renewal orders are counted as a separate order; modification orders and amendments are not counted.

Estimating the number of targets. The government’s methodology for counting PR/TT targets is similar to the methodology described above for counting targets of electronic surveillance and/or physical search. If the IC received authorization for the installation and use of a PR/TT device against the same target in four separate applications, the IC would count one target, not

four. Alternatively, if the IC received authorization for the installation and use of a PR/TT device against four targets in the same application, the IC would count four targets.

Estimating the number of unique identifiers. This statistic counts (1) the targeted identifiers and (2) the non-targeted identifiers (e.g., telephone numbers and e-mail addresses) that were in contact with the targeted identifiers. Specifically, the House Report on the USA FREEDOM Act states that "[t]he phrase 'unique identifiers used to communicate information collected pursuant to such orders' means the total number of, for example, email addresses or phone numbers that have been collected as a result of these particular types of FISA orders--not just the number of target email addresses or phone numbers." [H.R. Rept. 114-109 Part I, p. 26], with certain exceptions noted.

Figure 14: Table of PR/TT Orders, Targets, and Unique Identifiers Collected

<u>Title IV of FISA</u>					
<i>PR/TT FISA</i>	CY2013	CY2014	CY2015	CY2016	CY2017
Total number of orders	131	135	90	60	33
Estimated number of targets of such orders	319	516	456	41	27
Estimated number of unique identifiers used to communicate information collected pursuant to such orders*	-	-	134,987 [#]	81,035 ^{#†}	56,064[#]

See 50 U.S.C. §§ 1873(b)(3), 1873(b)(3)(A), and 1873(b)(3)(B).

* Pursuant to §1873(d)(2)(B), this statistic does not apply to orders resulting in the acquisition of information by the FBI that does not include electronic mail addresses or telephone numbers.

This number represents information the government received from provider(s) electronically for the entire calendar year. The government does not have a process for capturing unique identifiers received by other means (such as hard-copy or portable media).

† Last year, the FBI mistakenly interchanged the number of unique identifiers for business records and PR/TT orders, reporting the number of business records unique identifiers as PR/TT unique identifiers and vice versa. This report corrects the error and accurately identifies the legal authority under which the FBI obtained the unique identifiers.

Figure 15: Table of FISA PR/TT Targets – U.S. Persons and Non-U.S. Persons*

<u>PR/TT Targets</u>	CY2016	CY2017
Estimated number of targets who are <i>non</i> -U.S. persons	23	16
Estimated number of targets who are U.S. persons	18	11
Estimated percentage of targets who are U.S. persons	43.9%	40.7%

See 50 U.S.C. §§1873(b)(3)(A)(i) and 1873(b)(3)(A)(ii) for rows one and two, respectively.

* Previously the IC was not statutorily required to publicly provide these statistics, but provided them consistent with transparency principles. The reauthorized FAA of 2017 codified this requirement at 50 U.S.C. §§ 1873(b)(3)(A)(i) and 1873(b)(3)(A)(ii).

FISA Title V – Business Records

A. Business Records FISA

Under FISA, Title V authorizes the government to submit an application for an order requiring the production of any tangible things for (i) “an investigation to obtain foreign intelligence information not concerning a United States person or” (ii) “to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution.” 50 U.S.C. § 1861. Title V is commonly referred to as the “*Business Records*” provision of FISA.

In June 2015, the USA FREEDOM Act was signed into law and, among other things, it amended Title V, including by prohibiting bulk collection. See 50 U.S.C. §§ 1861(b), 1861(k)(4). The DNI is required to report various statistics about two Title V provisions – traditional business records and call detail records (discussed further below). On November 28, 2015, in compliance with amendments enacted by the USA FREEDOM Act, the IC terminated collection of bulk telephony metadata under Title V of the FISA (the “Section 215 Program”). Solely due to legal obligations to preserve records in certain pending civil litigation, including *First Unitarian Church of Los Angeles, et al. v. National Security Agency, et al.*, No. C 13-03287-JSW (N.D. Cal.) and *Jewel, et al. v. National Security Agency, et al.*, No. C 08-04373-JSW (N.D. Cal.), the IC continues to preserve previously collected bulk telephony metadata. Under the terms of a FISC order dated November 24, 2015, the bulk telephony metadata cannot be used or accessed for any purpose other than compliance with preservation obligations. Once the government’s preservation obligations are lifted, the government is required to promptly destroy all bulk metadata produced by telecommunications providers under the Section 215 Program.

FISA Title V

→ Commonly referred to as “*Business Records*” provision.

→ Bulk collection is prohibited.

→ Call Detail Records (CDRs) may be obtained from a telephone company if the FISC issues an individual court order for target’s records.

→ Request for records in an investigation of a U.S. person must be based on an investigation to protect against terrorism or clandestine intelligence activities and provided that the investigation is not conducted solely upon activities protected by the First Amendment to the Constitution.

As noted in last year's *Annual Statistical Transparency Report*, on November 30, 2015, the IC implemented certain provisions of the USA FREEDOM Act, including the call detail records provision and the requirement to use a specific selection term. Accordingly, only one month's worth of data for calendar year 2015 was available with respect to those provisions. Any statistical information relating to a particular FISA authority for a particular month remains classified. Therefore, the Title V data specifically associated with December 2015 was only released in a classified annex provided to Congress as part of the report for CY2015. For the CY 2016 report, statistical information was collected for an entire year under the USA FREEDOM Act Title V provisions. As a result, those statistics were included in that report. For the CY 2017 report, statistical information was collected for an entire year under the USA FREEDOM Act Title V provisions. As a result, those statistics are included in this report.

Statistics related to *traditional business records* under Title V Section 501(b)(2)(B) are provided first pursuant to 50 U.S.C. § 1873(b)(5). Statistics related to *call detail records* under Title V Section 501(b)(2)(C) are provided second pursuant to 50 U.S.C. § 1873(b)(6).

B. Statistics – “Traditional” Business Records Statistics Orders, Targets & Identifiers

Business Record (BR) requests for tangible things include books, records, papers, documents, and other items pursuant to 50 U.S.C. §1861(b)(2)(B), also referred to as Section 501(b)(2)(B) . These are commonly referred to as “Traditional” Business Records.

Estimating the number of unique identifiers. This is an estimate of the number of (1) targeted identifiers (e.g., telephone numbers and email addresses) and (2) non-targeted identifiers that were in contact with the targeted identifiers. This metric represents unique identifiers received electronically from the provider(s). The government does not have a process for capturing unique identifiers received by other means (i.e., hard-copy or portable media).

Explaining how we count BR statistics. As an example of the government's methodology, assume that in 2017, the government submitted a BR request targeting “John Doe” with email addresses john.doe@serviceproviderX, john.doe@serviceproviderY, and john.doe@serviceproviderZ. The FISC found that the application met the requirements of Title V and issued orders granting the application and directing service providers X, Y, and Z to produce business records pursuant to Section 501(b)(2)(B). Provider X returned 10 non-targeted email addresses that were in contact with the target; provider Y returned 10 non-targeted email addresses that were in contact with the target; and provider Z returned 10 non-targeted email addresses that were in contact with the target. Based on this scenario, we would report the following statistics: A) one order by the FISC for the production of tangible things, B)

one target of said orders, and C) 33 unique identifiers, representing three targeted email addresses plus 30 non-targeted email addresses.

Figure 16: Table of “Traditional” Business Records Orders, Targets, and Unique Identifiers Collected

Business Records “BR” – Section 501(b)(2)(B)	CY2016	CY2017
Total number of orders issued pursuant to applications under Section 501(b)(2)(B)	84	77
Estimated number of targets of such orders	88	74
Estimated number of unique identifiers used to communicate information collected pursuant to such orders	125,354†	87,834

See 50 U.S.C. §§ 1873(b)(5), 1873(b)(5)(A), and 1873(b)(5)(B).

† Last year, the FBI mistakenly interchanged the number of unique identifiers for business records and PR/TT orders, reporting the number of business records unique identifiers as PR/TT unique identifiers and vice versa. This report corrects the error and accurately identifies the legal authority under which the FBI obtained the unique identifiers.

C. Statistics – Call Detail Record (CDR) Orders, Targets & Identifiers

Call Detail Records (CDRs) – commonly referred to as “call event metadata” – may be obtained from traditional telecommunications providers pursuant to 50 U.S.C. §1861(b)(2)(C). A CDR is defined as session identifying information (such as originating or terminating telephone number, an International Mobile Subscriber Identity (IMSI) number, or an International Mobile Station Equipment Identity (IMEI) number), a telephone calling card number, or the time or duration of a call. See 50 U.S.C. §1861(k)(3)(A). CDRs provided to the government do not include the content of any communication, the name, address, or financial information of a subscriber or customer, or cell site location or global positioning system information. See 50 U.S.C. §1861(k)(3)(B). CDRs are stored and queried by the service providers. See 50 U.S.C. §1861(c)(2).

Estimating the number of targets of CDR orders. A “target” is the person using the selector. For example, if a target uses four selectors that have been approved, the number counted for purposes of this report would be one target, not four. Alternatively, if two targets are using one selector that has been approved, the number counted would be two targets.

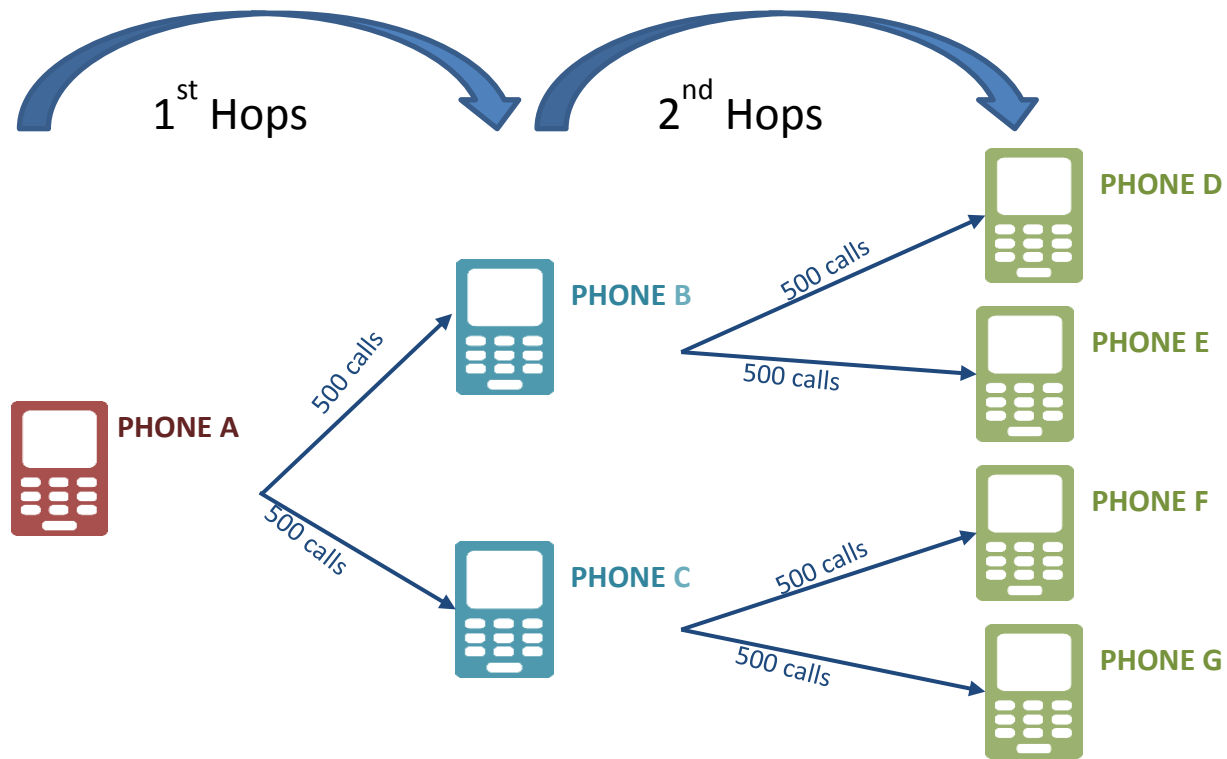
Figure 17: Table of CDR Orders and Targets

Call Detail Records “CDRs” – Section 501(b)(2)(C)	CY2016	CY2017
Total number of orders issued pursuant to applications under Section 501(b)(2)(C)	40	40
Estimated number of targets of such orders	42	40

See 50 U.S.C. §§ 1873(b)(6) and 1873(b)(6)(A).

The estimated number of Call Detail Records received from providers. This metric represents the number of *records received* from the provider(s) and stored in NSA repositories (records that fail at any of a variety of validation steps are not included in this number). CDRs covered by § 501(b)(2)(C) include call detail records created before, on, or after the date of the application relating to an authorized investigation. While the USA FREEDOM Act directs the government to provide a good faith estimate of “the number of unique identifiers used to communicate information collected pursuant to” orders issued in response to CDR applications (*see* 50 U.S.C. § 1873(b)(5)(B)), the statistic below does *not* reflect the number of unique identifiers contained within the call detail records received from the providers. As of the date of this report, the government does not have the technical ability to isolate the number of unique identifiers within records received from the providers. As explained in the [2016 NSA public report on the USA FREEDOM Act](#), the metric provided is over-inclusive because the government counts each record *separately even if the government receives the same record multiple times* (whether from one provider or multiple providers). Additionally, this metric includes duplicates of unique identifiers – i.e., because the government lacks the technical ability to isolate unique identifiers, the statistic counts the number of records even if unique identifiers are repeated. For example, if one unique identifier is associated with multiple calls to a second unique identifier, it will be counted multiple times. Similarly, if two different providers submit records showing the same two unique identifiers in contact, then those would also be counted. This statistic includes records that were received from the providers in CY2017 for all orders active for any portion of the year, which includes orders that the FISC approved in 2016. Furthermore, while the records are received from domestic communications service providers, the records received are for domestic and foreign numbers. More information on how NSA implements this authority can be found in the DCLPO report, in particular [see page 5 for a description and illustration of the USA FREEDOM Implementation Architecture](#).

Figure 18: Illustration of a hop scenario and counting



Target uses Phone A which is the FISC-approved selector in the FISC order. This would count as **1 order, 1 target, 7 unique identifiers** (phones A, B, C, D, E, F, G) and, assuming 500 calls between parties, **6000 CDRs** (*produced for both sides of a call event).

Assume an NSA intelligence analyst learns that phone number (**Phone A**) is being used by a suspected international terrorist (target). **Phone A** is the “specific selection term” or “selector” that will be submitted to the FISC (or the Attorney General in an emergency) for approval using the “reasonable articulable suspicion” (RAS) standard. Assume that one provider (provider X) submits a record showing **Phone A** called unique identifier **Phone B** – what is referred to as a “call event.” This is the “**first hop.**” In turn, assume that NSA submits the “first-hop” Phone B to the provider X, and finds that unique identifier was used to call another unique identifier **Phone D**. This is the “**second-hop.**” If the unique identifiers call one another multiple times, then multiple CDRs are produced and duplication occurs. Additionally, the government may receive multiple CDRs for a single call event. NSA may also submit the specific selection Phone A number to another provider (provider Y) who may have CDRs of the same call events.

Not all CDRs provided to the government will be domestic numbers. The targeted “specific selection term” could be a foreign number, could have called a foreign number or the “first-

hop” number could have called a foreign number; thus, these CDRs statistics contain both domestic and foreign number results.

Figure 19: Table of CDRs Received Arising from Such Targets

Call Detail Records “CDRs” – Section 501(b)(2)(C)	CY2016	CY2017
Estimated number of call detail records arising from such targets that NSA received from providers pursuant to Section 501(b)(2)(C) and stored in its repositories*	151,230,968	534,396,285

* While the statute directs the government to count the unique identifiers, the government is not technically able to isolate the number of unique identifiers; thus, this number includes duplicate records. Additionally, the number of records contains both domestic and foreign numbers.

D. Statistics – Call Detail Record Queries

The number of search terms associated with a U.S. person used to query the CDR data. Each unique query is counted only once. The same term queried 10 times counts as one query term. A single query with 20 terms counts as 20 query terms.

Figure 20: Table of CDRs -- U.S. person query terms

Call Detail Records “CDRs” – Section 501(b)(2)(C)	CY2016	CY2017
Estimated number of search terms that included information concerning a U.S. person that were used to query any database of call detail records obtained through the use of such orders*	22,360	31,196

See 50 U.S.C. § 1873(b)(6)(C).

* Consistent with § 1873(d)(2)(A), this statistic does not include queries that are conducted by the FBI.

National Security Letters (NSLs)

A. National Security Letters

In addition to statistics relating to FISA authorities, we are reporting information on the government's use of National Security Letters (NSLs). The FBI is statutorily authorized to issue NSLs for specific records (as specified below) only if the information being sought is relevant to a national security investigation. NSLs may be issued for four commonly used types of records:

- 1) telephone subscriber information, toll records, and other electronic communication transactional records, see 18 U.S.C. § 2709;
- 2) consumer-identifying information possessed by consumer reporting agencies (names, addresses, places of employment, institutions at which a consumer has maintained an account), see 15 U.S.C. § 1681u;
- 3) full credit reports, see 15 U.S.C. § 1681v (only for counterterrorism, not for counterintelligence investigations); and
- 4) financial records, see 12 U.S.C. § 3414.

National Security Letters

→ Not authorized by FISA but by other statutes.

→ Bulk collection is prohibited, however, by the USA FREEDOM Act.

→ FBI may only use NSLs if the information sought is relevant to international counterterrorism or counterintelligence investigation.

B. Statistics – National Security Letters and Requests of Information

Counting NSLs. Today we are reporting (1) the total number of NSLs *issued* for all persons, and (2) the total number of requests for information (ROI) contained within those NSLs. When a single NSL contains multiple ROIs, each is considered a “request” and each request must be relevant to the same pending investigation. For example, if the government issued one NSL seeking subscriber information from one provider and that NSL identified three e-mail addresses for the provider to return records, this would count as one NSL issued and three ROIs.

- **The Department of Justice’s Report on NSLs.** In May 2018, the Department of Justice released its [Annual Foreign Intelligence Surveillance Act Report](#) to Congress. That report, which is available online, provides the *number of requests* made for certain information concerning different U.S. persons pursuant to NSL authorities during calendar year 2017. The Department of Justice’s report provides the number of individuals subject to an NSL whereas the ODNI’s report provides the number of NSLs issued. Because one person may be subject to more than one NSL in an annual period, the number of NSLs issued and the number of persons subject to an NSL differs.

Why we report the number of NSL requests instead of the number of NSL targets. We are reporting the annual number of requests for multiple reasons. First, the FBI’s systems are configured to comply with Congressional reporting requirements, which do not require the FBI to track the number of individuals or organizations that are the subject of an NSL. Even if the FBI systems were configured differently, it would still be difficult to identify the number of specific individuals or organizations that are the subjects of NSLs. One reason for this is that the subscriber information returned to the FBI in response to an NSL may identify, for example, one subscriber for three accounts or it may identify different subscribers for each account. In some cases this occurs because the identification information provided by the subscriber to the provider may not be true. For example, a subscriber may use a fictitious name or alias when creating the account. Thus, in many instances, the FBI never identifies the actual subscriber of a facility. In other cases, this occurs because individual subscribers may identify themselves differently for each account (e.g., inclusion of middle name, middle initial, etc.) when creating an account.

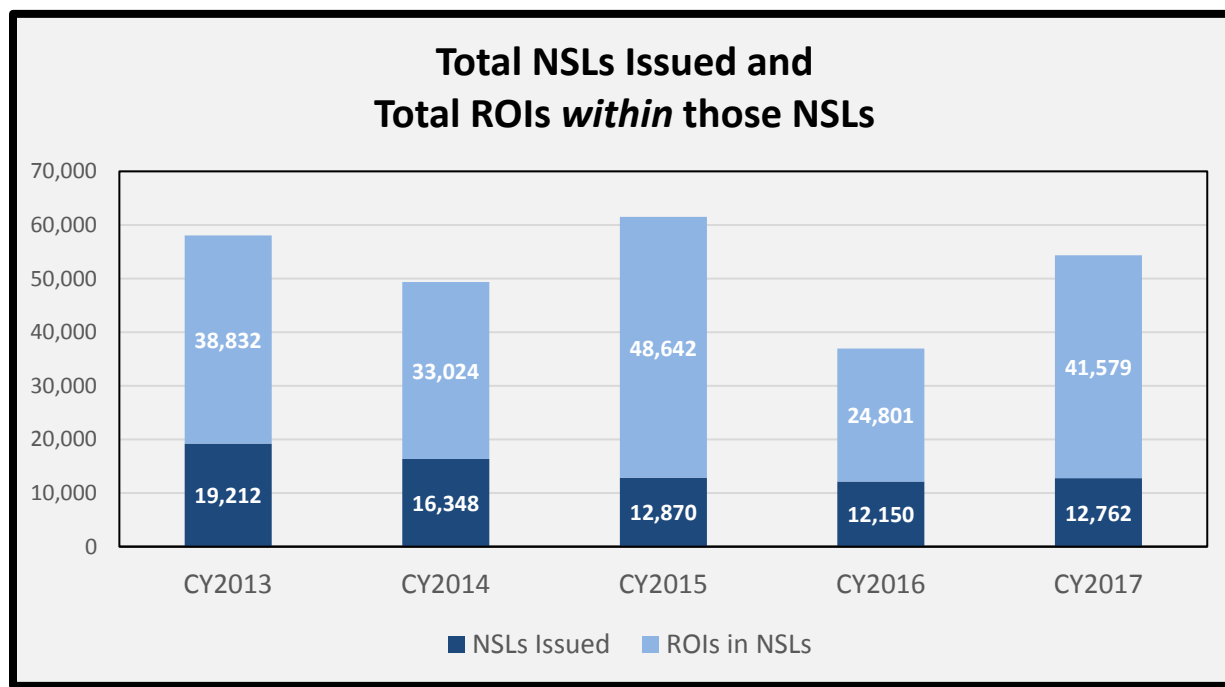
We also note that the actual number of individuals or organizations that are the subject of an NSL is different than the number of NSL requests. The FBI often issues NSLs under different legal authorities, e.g., 12 U.S.C. § 3414(a)(5), 15 U.S.C. §§ 1681u(a) and (b), 15 U.S.C. § 1681v, and 18 U.S.C. § 2709, for the same individual or organization. The FBI may also serve multiple NSLs for an individual for multiple facilities (e.g., multiple e-mail accounts, landline telephone numbers and cellular phone numbers). The number of requests, consequently, is significantly larger than the number of individuals or organizations that are the subjects of the NSLs.

Figure 21a: Table of NSLs Issued and Requests for Information

<u>National Security Letters (NSLs)</u>	CY2013	CY2014	CY2015	CY2016	CY2017
Total number of NSLs issued	19,212	16,348	12,870	12,150	12,762
Number of Requests for Information (ROI)	38,832	33,024	48,642	24,801	41,579

See 50 U.S.C. § 1873(b)(6).

Figure 21b: Chart of NSLs Issued and Requests for Information



APPENDIX

UNCLASSIFIED

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

MAY 04 2018

The Honorable Richard Burr
Chairman
Select Committee on Intelligence
United States Senate

The Honorable Chuck Grassley
Chairman
Committee on the Judiciary
United States Senate

The Honorable Devin Nunes
Chairman
Permanent Select Committee on Intelligence
U.S. House of Representatives

The Honorable Robert W. Goodlatte
Chairman
Committee on the Judiciary
U.S. House of Representatives

Dear Messrs. Chairmen:

Section 603(b)(2)(B) of the Foreign Intelligence Surveillance Act (FISA), as amended by the *Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015*, (P.L. 114-23), 129 Stat. 268 (hereinafter USA FREEDOM Act), requires the Director of National Intelligence (DNI) to make publicly available for the preceding 12-month period a good faith estimate of the number of queries concerning a known United States person of unminimized non-content information relating to electronic communications or wire communications obtained through acquisitions authorized under Section 702 of FISA, excluding the number of queries containing information used to prevent the return of information concerning a United States person.

If the DNI concludes that this good faith estimate cannot be determined accurately because not all of the relevant elements of the Intelligence Community (IC) are able to provide this good faith estimate, then FISA requires him to (i) certify that conclusion in writing to the committees identified above; (ii) report the good faith estimate for those relevant elements able to provide such good faith estimate; (iii) explain when it is reasonably anticipated that such an estimate will be able to be determined fully and accurately; and (iv) make such certification publicly available on an Internet website.

I conclude that the good faith estimate required under section 603(b)(2)(B) of FISA cannot be determined accurately because not all of the relevant elements of the IC are able to provide this good faith estimate. Specifically, the Central Intelligence Agency (CIA) remained unable to provide such information for calendar year 2017. The enclosed report includes the good faith estimate for those relevant IC elements that were able to provide such good faith estimate. Based on the information provided to me by the CIA, I reasonably anticipate that such an estimate will be able to be determined fully and accurately by the end of calendar year 2018 so as to be included in the 2019 report.

UNCLASSIFIED

JA2788

UNCLASSIFIED

The Honorable Richard Burr
The Honorable Chuck Grassley
The Honorable Devin Nunes
The Honorable Robert W. Goodlatte

If you have any questions regarding this matter, please contact the Office of the Director of National Intelligence Office of Legislative Affairs at (703) 275-2474.

Sincerely,



Daniel R. Coats

Enclosure:
Statistical Transparency Report

cc: Executive Secretary, National Security Staff
Director, Central Intelligence Agency
Under Secretary of Defense for Intelligence
Under Secretary for Intelligence and Analysis, Department of Homeland Security
Director, National Security Agency
Director, National Reconnaissance Office
Director, Defense Intelligence Agency
Director, National Geospatial-Intelligence Agency
Assistant Secretary for Intelligence and Research, Department of State
Assistant Secretary for Intelligence and Analysis, Department of the Treasury
Executive Assistance Director, Intelligence Branch, Federal Bureau of Investigation
Chief of Intelligence, Senior Officer, Drug Enforcement Administration
Director, Office of Intelligence and Counterintelligence, Department of Energy
Deputy Chief of Staff, G2, U.S. Army
Director of Intelligence, U.S. Marine Corps
Director of Naval Intelligence, N2 U.S. Navy
Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance, A2, U.S. Air Force
Deputy Chief of Staff for Intelligence and Criminal Investigations, U.S. Coast Guard
Assistant Attorney General for National Security, Department of Justice

UNCLASSIFIED

JA2789

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 21

Filed
United States Foreign
Intelligence Surveillance Court

APR 26 2017

LeeAnn Flynn Hall, Clerk of Court

~~TOP SECRET//SI//ORCON/NOFORN~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.



MEMORANDUM OPINION AND ORDER

These matters are before the Foreign Intelligence Surveillance Court (“FISC” or “Court”) on the “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,” which was filed on September 26, 2016 (“September 26, 2016 Submission”), and the “Government’s Ex Parte Submission of Amendments to DNI/AG 702(g) Certifications and Ex Parte Submission of Amended Targeting and Minimization Procedures,” which was filed on March 30, 2017 (“March 30, 2017 Submission”). (Collectively, the September 26, 2016 and March 30, 2017 Submissions will be

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

referred to herein as the “2016 Certification Submissions.”) For the reasons explained below, the government’s request for approval of the certifications and procedures accompanying the September 26, 2016 Submission, as amended by the March 30, 2017 Submission, is granted, subject to certain reporting requirements. The Court’s approval of the amended certifications and accompanying targeting and minimization procedures is set out in separate orders, which are being entered contemporaneously herewith.

I. BACKGROUND

A. The Initial 2016 Certifications

The September 26, 2016 Submission included [REDACTED] certifications that were executed by the Attorney General (“AG”) and the Director of National Intelligence (“DNI”) pursuant to Section 702 of the Foreign Intelligence Surveillance Act (“FISA” or “the Act”), which is codified at 50 U.S.C. § 1881a [REDACTED]

[REDACTED] Each of the [REDACTED] certifications submitted in September (collectively referred to as “the Initial 2016 Certifications”) was accompanied by the supporting affidavits of the Director of the National Security Agency (“NSA”), the Director of the Federal Bureau of Investigation (“FBI”), the Director of the Central Intelligence Agency (“CIA”), and the Director of the National Counterterrorism Center (“NCTC”); two sets of targeting procedures, for use by the NSA and FBI respectively;¹ and four sets of minimization procedures, for use by the

¹ The targeting procedures for each of the Initial 2016 Certifications are identical. The (continued...)

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 2

~~TOP SECRET//SI//ORCON//NOFORN~~

NSA, FBI, CIA, and NCTC respectively.² The September 26, 2016 Submission also included an explanatory memorandum prepared by the Department of Justice (“DOJ”) (“September 26, 2016 Memorandum”).

The Court was required to complete its review of the Initial 2016 Certifications within 30 days of their submission, i.e., by October 26, 2016. See 50 U.S.C. § 1881a(i)(1)(B). The Court may extend this period, however, “as necessary for good cause in a manner consistent with national security.” See 50 U.S.C. § 1881a(j)(2). The Court has issued two such extensions in these matters.

¹(...continued)

targeting procedures for the NSA (“NSA Targeting Procedures”) appear as Exhibit A to each of the 2016 Certifications and the March 30, 2017 Submission includes identical amendments to those procedures for each of the certifications. (Unless otherwise specified, references to those targeting procedures shall refer to the procedures as amended, as discussed below, in the March 30, 2017 Submission.) The targeting procedures for the FBI (“FBI Targeting Procedures”) appear as Exhibit C to each of the 2016 Certifications and are not amended by the March 30, 2017 Submission.

² The minimization procedures for each of the Initial 2016 Certifications are identical. The minimization procedures for the NSA (“NSA Minimization Procedures”) appear as Exhibit B to each of the 2016 Certifications and the March 30, 2017 Submission includes identical amendments to those procedures for each of the certifications. (Unless otherwise specified, references to those minimization procedures shall refer to the procedures as amended, as discussed below, in the March 30, 2017 Submission.) The minimization procedures for the FBI (“FBI Minimization Procedures”) appear as Exhibit D to each of the 2016 Certifications. The minimization procedures for the CIA (“CIA Minimization Procedures”) appear as Exhibit E to each of the 2016 Certifications. The minimization procedures for the NCTC (“NCTC Minimization Procedures”) appear as Exhibit G to each of the 2016 Certifications. The minimization procedures for the FBI, CIA, and NCTC are not amended by the March 30, 2017 Submission.

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 3

~~TOP SECRET//SI//ORCON/NOFORN~~

On October 24, 2016, the government orally apprised the Court of significant non-compliance with the NSA's minimization procedures involving queries of data acquired under Section 702 using U.S. person identifiers. The full scope of non-compliant querying practices had not been previously disclosed to the Court. Two days later, on the day the Court otherwise would have had to complete its review of the certifications and procedures, the government made a written submission regarding those compliance problems, see October 26, 2016, Preliminary and Supplemental Notice of Compliance Incidents Regarding the Querying of Section 702-Acquired Data ("October 26, 2016 Notice"), and the Court held a hearing to address them. The government reported that it was working to ascertain the cause(s) of those compliance problems and develop a remedial plan to address them. Without further information about the compliance problems and the government's remedial efforts, the Court was not in a position to assess whether the minimization procedures accompanying the Initial 2016 Certifications, as they would be implemented, would comply with statutory standards and were consistent with the requirements of the Fourth Amendment. See 50 U.S.C. § 1881a(i)(3)(A)-(B). Accordingly, the Court found good cause to extend the time limit for its review of the Initial 2016 Certifications through January 31, 2017, and, based on the government's representations, found that such extension was consistent with national security.³ See Docket Nos. [REDACTED]

[REDACTED] Order entered on Oct. 26, 2016 ("October 26, 2016 Order").

³ By operation of the statute, the predecessors to each of the Initial 2016 Certifications and the procedures accompanying them remained in effect during the extended periods for the Court's consideration of the 2016 Certifications. See 50 U.S.C. § 1881a(i)(3)(A)-(B).

~~TOP SECRET//SI//ORCON/NOFORN~~

Page 4

JA2794

~~TOP SECRET//SI//ORCON//NOFORN~~

On January 3, 2017, the government made a further submission describing its efforts to ascertain the scope and causes of those compliance problems and discussing potential solutions to them. See January 3, 2017, Supplemental Notice of Compliance Incidents Regarding the Querying of Section 702-Acquired Data (“January 3, 2017 Notice”). The Court was not satisfied that the government had sufficiently ascertained the scope of the compliance problems or developed and implemented adequate solutions for them and communicated a number of questions and concerns to the government. The government submitted another update on January 27, 2017, in which it informed the Court that, due to the complexity of the issues involved, NSA would not be in a position to provide thorough responses to the Court’s questions and concerns by January 31, 2017. See January 27, 2017, Letter In re: DNI/AG 702(g) Certifications [REDACTED] and their Predecessor Certifications (“January 27, 2017 Letter”). The government submitted that a further extension, through May 26, 2017, was necessary for it to address those issues and that such extension would be consistent with national security. The Court granted a shorter extension, through April 28, 2017, for reasons stated in its order approving the extension. See Docket Nos. [REDACTED] Order entered on Jan. 27, 2017 (“January 27, 2017 Order”).

B. The 2017 Amendments

On March 30, 2017, the Attorney General and Director of National Intelligence, acting pursuant to 50 U.S.C. § 1881a(i)(1)(C), executed Amendments to each of the [REDACTED] Initial 2016 Certifications. See Amendment to [REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 5

JA2795

~~TOP SECRET//SI//ORCON//NOFORN~~

[REDACTED]

(collectively, the “2017 Amendments”).⁴ As discussed below, those amendments substantially change how NSA will conduct certain aspects of Section 702 collection, and largely resolve the compliance problems mentioned above. The March 30, 2017 Submission included the 2017 Amendments, a revised supporting affidavit by the Director of NSA, and revised targeting and minimization procedures for NSA, which replace Exhibits A and B, respectively, to each of the Initial 2016 Certifications. That submission also included an explanatory memorandum prepared by DOJ (“March 30, 2017 Memorandum”).

C. Subject Matter of the Certifications

Each of the 2016 Certifications involves “the targeting of non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information.”

[REDACTED]

⁴ Unless otherwise stated, subsequent references to the “2016 Certifications” are to the Initial 2016 Certifications and accompanying procedures, as later amended by the 2017 Amendments and the accompanying revised procedures.

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 6

JA2796

~~TOP SECRET//SI//ORCON//NOFORN~~

Each of the 2016 Certifications generally proposes to continue acquisitions of foreign intelligence information that are now being conducted under the corresponding certification made in 2015 (“the 2015 Certifications”). See September 26, 2016 Memorandum at 2. The 2015 Certifications, which are similarly differentiated by subject matter and [REDACTED] [REDACTED] were approved by the FISC on November 6, 2015.⁵ The 2015 Certifications, in turn, generally renewed authorizations to acquire foreign intelligence information under a series of certifications made by the AG and DNI pursuant to Section 702 that dates back to 2008.⁶ The government also seeks approval of amendments to the certifications in the Prior 702 Dockets, such that the NSA, CIA, FBI and NCTC henceforward will apply the same minimization

⁵ See Docket Nos. [REDACTED] Memorandum Opinion and Order entered on Nov. 6, 2015 (“November 6, 2015 Opinion”). The Court issued an order on November 9, 2015, approving amendments to prior Section 702 certifications and authorizing the use of revised minimization procedures in connection with those certifications.

⁶ See Docket Nos. [REDACTED]

[REDACTED] These dockets, together with Docket Numbers [REDACTED] are collectively referred to as “the Prior 702 Dockets.”

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 7

~~TOP SECRET//SI//ORCON/NOFORN~~

procedures to information obtained under prior certifications as they will to information to be obtained under the 2016 Certifications. See September 26, 2016 Memorandum at 2-3;

[REDACTED]

This practice, long approved by the FISC, has the advantage of applying a single set of updated procedures to Section 702-acquired information rather than requiring personnel to follow different rules for information acquired on different dates.

D. Review of Compliance Issues

The Court's review of targeting and minimization procedures under Section 702 is not confined to the procedures as written; rather, the Court also examines how the procedures have been and will be implemented. See, e.g., Docket No. [REDACTED], Memorandum Opinion entered on Apr. 7, 2009, at 22-24 ("April 7, 2009 Opinion"); Docket Nos. [REDACTED] [REDACTED] Memorandum Opinion entered on Aug. 30, 2013, at 6-11 ("August 30, 2013 Opinion"). Accordingly, for purposes of its review of the 2016 Certifications, the Court has examined quarterly compliance reports submitted by the government since the most recent FISC review of Section 702 certifications and procedures was completed on November 6, 2015,⁷ as well as individual notices of non-compliance relating to implementation of Section 702. The Court held a hearing on October 4, 2016, to address certain issues raised by the September 26,

⁷ See Quarterly Reports to the FISC Concerning Compliance Matters Under Section 702 of FISA, submitted on December 18, 2015, March 18, 2016, June 17, 2016, September 16, 2016, December 16, 2016 and March 17, 2017. These reports are cited herein in the form "[Date] Compliance Report."

~~TOP SECRET//SI//ORCON/NOFORN~~

Page 8

~~TOP SECRET//SI//ORCON//NOFORN~~

2016 Submission, as well as certain compliance issues regarding the government's collection and handling of information under prior certifications ("October 4, 2016 Hearing").⁸ The Court held a further hearing on October 26, 2016, to address matters raised in the October 26, 2016 Notice ("October 26, 2016 Hearing").⁹

II. REVIEW OF CERTIFICATIONS [REDACTED] AND OF THEIR PREDECESSOR CERTIFICATIONS AS AMENDED BY THE SEPTEMBER 26, 2016 AND MARCH 30, 2017 SUBMISSIONS

The Court must review a certification submitted pursuant to Section 702 "to determine whether [it] contains all the required elements." 50 U.S.C. § 1881a(i)(2)(A). The Court's examination of Certifications [REDACTED] as amended by the 2017 Amendments, confirms that:

(1) the certifications have been made under oath by the AG and the DNI, as required by 50 U.S.C. § 1881a(g)(1)(A), see [REDACTED]

(2) the certifications contain each of the attestations required by 50 U.S.C. § 1881a(g)(2)(A), see [REDACTED]

(3) as required by 50 U.S.C. § 1881a(g)(2)(B), each of the certifications is accompanied by the applicable targeting procedures and minimization procedures;

⁸ See generally Transcript of Proceedings Held Before the Honorable Rosemary M. Collyer on October 4, 2016 ("October 4, 2016 Transcript").

⁹ See generally Transcript of Proceedings Held Before the Honorable Rosemary M. Collyer on October 26, 2016 ("October 26, 2016 Transcript").

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 9

~~TOP SECRET//SI//ORCON/NOFORN~~

(4) each of the certifications is supported by the affidavits of appropriate national security officials, as described in 50 U.S.C. § 1881a(g)(2)(C);¹⁰ and

(5) each of the certifications includes an effective date for the authorization in compliance with 50 U.S.C. § 1881a(g)(2)(D) – specifically, the certifications become effective on April 28, 2017, or on the date upon which this Court issues an order concerning the certifications under Section 1881a(i)(3), whichever is sooner, see [REDACTED]

¹¹

The Court therefore finds that [REDACTED]

[REDACTED] contain all the required statutory elements. See 50 U.S.C. § 1881a(i)(2)(A).

Similarly, the Court has reviewed the certifications in the Prior 702 Dockets, as amended by the 2016 Certifications, and finds that they also contain all the elements required by the statute. Id.¹²

¹⁰ See Affidavits of Admiral Michael S. Rogers, United States Navy, Director, NSA; Affidavits of James B. Comey, Director, FBI; Affidavits of John O. Brennan, Director, CIA; and Affidavits of Nicholas Rasmussen, Director, NCTC, which are appended to each of Certifications [REDACTED]. Admiral Rogers filed amended affidavits in connection with the March 30, 2017 Submission.

¹¹ The statement described in 50 U.S.C. § 1881a(g)(2)(E) is not required in this case because there has been no “exigent circumstances” determination under Section 1881a(c)(2).

¹² The effective dates for the amendments to the certifications in the Prior 702 Dockets are the same as the effective dates for the 2016 Certifications. See [REDACTED]

~~TOP SECRET//SI//ORCON/NOFORN~~

Page 10

JA2800

~~TOP SECRET//SI//ORCON//NOFORN~~

III. REVIEW OF THE TARGETING AND MINIMIZATION PROCEDURES

The Court is also required, pursuant to 50 U.S.C. § 1881a(i)(2)(B) and (C), to review the targeting and minimization procedures to determine whether they are consistent with the requirements of 50 U.S.C. § 1881a(d)(1) and (e)(1). Pursuant to 50 U.S.C. § 1881a(i)(3)(A), the Court further assesses whether the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment.

A. Statutory Standards for Targeting Procedures

Section 1881a(d)(1) requires targeting procedures that are “reasonably designed” to “ensure that any acquisition authorized under [the certification] 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.” In addition to these statutory requirements, the government uses the targeting procedures as a means of complying with Section 1881a(b)(3), which provides that acquisitions “may not intentionally target a United States person reasonably believed to be located outside the United States.” The FISC considers steps taken pursuant to these procedures to avoid targeting United States persons as relevant to its assessment of whether the procedures are consistent with the requirements of the Fourth Amendment. See Docket No. 702(i)-08-01, Memorandum Opinion entered on Sept. 4, 2008, at 14 (“September 4, 2008 Opinion”).

Under the procedures adopted by the government, NSA is the lead agency in making targeting decisions under Section 702. Pursuant to its targeting procedures, NSA may target for

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 11

~~TOP SECRET//SI//ORCON/NOFORN~~

acquisition a particular “selector,” which is typically a facility such as a telephone number or e-mail address. The FBI Targeting Procedures come into play in cases where [REDACTED]

[REDACTED] that has been tasked under the NSA Targeting Procedures. See FBI Targeting Procedures § I.1. “Thus, the FBI Targeting Procedures apply in addition to the NSA Targeting Procedures, whenever [REDACTED] acquired.”

September 4, 2008 Opinion at 20 (emphasis in original). Proposed changes to the existing NSA and FBI targeting procedures are discussed below.

B. Statutory Standards for Minimization Procedures

Section 1881a(e)(1), in turn, requires minimization procedures that “meet the definition of minimization procedures under [50 U.S.C. §] 1801(h) or 1821(4).” Sections 1801(h) and 1821(4) define “minimization procedures” in pertinent part as:

(1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance [or physical search], 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;^[13]

¹³ Section 1801(e) defines “foreign intelligence information” as

(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

(continued...)

~~TOP SECRET//SI//ORCON/NOFORN~~

Page 12.

~~TOP SECRET//SI//ORCON//NOFORN~~

(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in [50 U.S.C. § 1801(e)(1)], shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance; [and]

(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes[.]

50 U.S.C. § 1801(h); see also id. § 1821(4).¹⁴ Each agency having access to “raw,” or unminimized,¹⁵ information obtained under Section 702 is governed by its own set of

¹³(...continued)

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 a 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.

¹⁴ The definitions of “minimization procedures” set forth in these provisions are substantively identical (although Section 1821(4)(A) refers to “the purposes . . . of the particular physical search”). For ease of reference, subsequent citations refer only to the definition set forth at Section 1801(h).

¹⁵ This opinion uses the terms “raw” and “unminimized” interchangeably. The proposed NCTC Minimization Procedures define “raw” information as “section 702-acquired information that (i) is in the same or substantially the same format as when NSA or FBI acquired it, or (ii) has been processed only as necessary to render it into a form in which it can be evaluated to

(continued...)

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 13

~~TOP SECRET//SI//ORCON/NOFORN~~

minimization procedures in its handling of Section 702 information. Under Section 1881a(i)(2)(C), the Court must determine whether the agencies' respective minimization procedures meet the statutory definition of minimization procedures set forth at 50 U.S.C. §§ 1801(h) or 1821(4), as appropriate.

The most significant changes to the procedures proposed by the government in connection with the 2016 Certifications relate to: (i) the changes in the scope of NSA collection under Section 702, as reflected in the March 30, 2017 Amendments; and (ii) the government's proposal in the September 26, 2016 Submission to allow NCTC access to unminimized information acquired by NSA and FBI [REDACTED] [REDACTED] relating to international terrorism [REDACTED].

Because those changes cut across several sets of procedures, each is discussed individually in a separate section. This opinion then examines several other changes to various sets of procedures proposed by the government in the September 26, 2016 Submission. The opinion then will assess whether, taken as a whole and including the proposed changes, the proposed targeting and minimization procedures satisfy applicable statutory and Fourth Amendment requirements.

C. Significant Changes to NSA Targeting and Minimization Procedures in the March 30, 2017 Submission

The October 26, 2016 Notice disclosed that an NSA Inspector General (IG) review and report and NSA Office of Compliance for Operations (OCO) verification activities indicated that,

¹⁵(...continued)
determine whether it reasonably appears to be foreign intelligence information or to be necessary to understand foreign intelligence information or assess its importance." NCTC Minimization Procedures § A.3.d.

~~TOP SECRET//SI//ORCON/NOFORN~~

Page 14

~~TOP SECRET//SI//ORCON//NOFORN~~

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. To understand why such queries were prohibited, and why this disclosure gave the Court substantial concern, some historical background is necessary.

1. Upstream Collection and the Acquisition of MCTs

“Upstream” collection of Internet communications refers to NSA’s interception of such communications as they transit the facilities of an Internet backbone carrier [REDACTED] [REDACTED] as distinguished from acquiring communications from systems operated by Internet service providers [REDACTED].¹⁶ Upstream Internet collection constitutes a small percentage of NSA’s overall collection of Internet communications under Section 702, *see, e.g.*, October 3, 2011 Memorandum Opinion at 23 n.21 (noting that, at that time, upstream Internet collection constituted only 9% of NSA’s Internet collection), but it has represented more than its share of the challenges in implementing Section 702.

In 2011, the government disclosed that, as part of its upstream collection of Internet transactions, NSA acquired certain “Multiple Communication Transactions” or “MCTs.”¹⁷

¹⁶ *See In re DNI/AG 702(g) Certifications* [REDACTED] [REDACTED] Memorandum Opinion, October 3, 2011 (“October 3, 2011 Memorandum Opinion”), at 5 n.3. For purposes of the discussion that follows, familiarity with that opinion is presumed. As discussed below, NSA does not share raw upstream collection (Internet or telephony) with any other agency.

¹⁷ NSA’s procedures define an Internet transaction as consisting of either a discrete communication (e.g., an individual e-mail) or multiple discrete communications obtained within
(continued...)

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 15

~~TOP SECRET//SI//ORCON/NOFORN~~

MCTs might take the form of [REDACTED] containing

multiple e-mail messages [REDACTED]

[REDACTED]. See March 30, 2017 Memorandum at 8 n.8. The term “active user” refers to the user of a communication service to or from whom the MCT is in transit when it is acquired (e.g., the user of an e-mail account [REDACTED])

Eventually, as discussed below, a complicated set of minimization rules was adopted for handling different types of MCTs, based on whether the active user was the target¹⁸ and, if not, the nationality and location (to the extent known) of the active user.

Moreover, NSA upstream collection acquired Internet communications that were to, from *or about* (i.e., containing a reference to) a selector tasked for acquisition under Section 702. As a result, upstream collection could acquire an entire MCT for which the active user was a non-target and that mostly pertained to non-targets, merely because a *single* discrete communication within the MCT was to, from *or contained a reference to* a tasked selector. Such acquisitions could take place even if the non-target active user was a U.S. person in the United States and the MCT contained a large number of domestic communications¹⁹ that did not pertain to the foreign

¹⁷(...continued)

an MCT. See NSA Targeting Procedures § I, at 2 n.1; NSA Minimization Procedures § 2(g).

¹⁸ With a narrow exception for [REDACTED] all users of a selector tasked for acquisition under Section 702 are considered targets. See March 30, 2017 Memorandum at 6 n.7.

¹⁹ In this opinion, “domestic communications” are communications in which the sender
(continued...)

~~TOP SECRET//SI//ORCON/NOFORN~~

Page 16

~~TOP SECRET//SI//ORCON/NOFORN~~

intelligence target who used the tasked selector. Because of those types of acquisitions particularly, upstream Internet collection was “more likely than other forms of Section 702 collection to contain information of or concerning United States persons with no foreign intelligence value.” November 6, 2015 Opinion at 25 n.21.

It should be noted, however, that not all MCTs in which the active user is a non-target are equally problematic; for example, some MCTs within that description may involve an active user who is a non-U.S. person outside the United States, and for that reason are less likely to contain a large volume of information about U.S. persons or domestic communications.

2. The 2011 Finding of Deficiency and Measures to Remedy the Deficiency

In its October 3, 2011 Memorandum Opinion, the Court found the NSA’s minimization procedures, proffered in connection with Section 702 certifications then under consideration, statutorily and constitutionally deficient with respect to their protection of U.S. person information within certain types of MCTs. See October 3, 2011 Memorandum Opinion at 49-80. In response to the Court’s deficiency finding, the government submitted amended minimization procedures that placed significant new restrictions on NSA’s retention, use, and dissemination of MCTs. Those procedures included a sequestration regime for more problematic categories of MCTs.²⁰ A shorter retention period was also put into place, whereby an MCT of any type could not be retained longer than two years after the expiration of the certification pursuant to which it

¹⁹(...continued)
and all intended recipients are in the United States.

²⁰ This sequestration regime is discussed in Section IV below in connection with an instance of NSA’s not complying with that regime.

~~TOP SECRET//SI//ORCON/NOFORN~~

Page 17

~~TOP SECRET//SI//ORCON/NOFORN~~

was acquired, unless applicable retention criteria were met. And, of greatest relevance to the present discussion, those procedures categorically prohibited NSA analysts from using known U.S.-person identifiers to query the results of upstream Internet collection. In substantial reliance on these and other changes, the Court approved the modified procedures for acquiring and handling MCTs. See *In re DNI/AG 702(g) Certifications* [REDACTED] [REDACTED] Memorandum Opinion, November 30, 2011 (“November 30, 2011 Memorandum Opinion”).

The Court also observed that one category of MCTs presented far fewer statutory and constitutional difficulties than the others:

[I]f the target is the active user, then it is reasonable to presume that all of the discrete communications within an MCT will be to or from the target. Although United States persons and persons in the United States may be party to any of those communications, NSA's acquisition of such communications is of less concern than the communications described in the [other] categories [of MCTs] because the communicants were in direct communication with a tasked facility, and the acquisition presumptively serves the foreign intelligence purpose of the collection.

October 3, 2011 Memorandum Opinion at 38. See also *id.* at 58 n.54 (“The government has also suggested that NSA may have limited capability, at the time of acquisition, to identify some MCTs as to which the “active user” is a tasked selector. To the extent that NSA is able to do so, such acquisitions *would be consistent with FISA and the Fourth Amendment* because all discrete communications within this class of MCTs would consist of communications to or from a tasked selector.”) (internal citation omitted, emphasis added); *id.* at 80 (finding that the

~~TOP SECRET//SI//ORCON/NOFORN~~

Page 18

JA2808

~~TOP SECRET//SI//ORCON//NOFORN~~

proposed NSA procedures, although deficient as applied to other forms of MCTs, were consistent with the statute and the Fourth Amendment as applied to “MCTs as to which the ‘active user’ is known to be a tasked selector”). That point is significant to the current matters: as discussed below, the 2016 Certifications only authorize acquisition of MCTs when the active user is the target of acquisition.

3. The October 26, 2016 Notice and Hearing

Since 2011, NSA’s minimization procedures have prohibited use of U.S.-person identifiers to query the results of upstream Internet collection under Section 702. The October 26, 2016 Notice informed the Court that NSA analysts had been conducting such queries in violation of that prohibition, with much greater frequency than had previously been disclosed to the Court. The Notice described the results of an NSA IG Report which analyzed queries using a set of known U.S.-person identifiers (those associated with targets under Sections 704 and 705(b) of the Act, 50 U.S.C. §§ 1881c and 1881d(b)), during the first three months of 2015, in a subset of particular NSA systems that contain the results of Internet upstream collection. That relatively narrow inquiry found that ■ analysts had made ■ separate queries using ■ U.S.-person identifiers that improperly ran against upstream Internet data. The government reported that the NSA IG and OCO were conducting other reviews covering different time periods, with preliminary results suggesting that the problem was widespread during all periods under review.

At the October 26, 2016 hearing, the Court ascribed the government’s failure to disclose those IG and OCO reviews at the October 4, 2016 hearing to an institutional “lack of candor” on NSA’s part and emphasized that “this is a very serious Fourth Amendment issue.” October 26,

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 19

~~TOP SECRET//SI//ORCON/NOFORN~~

2016 Transcript at 5-6. The Court found that, in light of the recent revelations, it did not have sufficient information to assess whether the proposed minimization procedures accompanying the Initial 2016 Certifications would comply with statutory and Fourth Amendment requirements, as implemented. Based on the government's representation that an extension of time through January 31, 2017, would provide the government sufficient opportunity to assess and report on the scope of the problem and an appropriate remedial plan, and was consistent with the national security, the Court extended the time period for its consideration of the 2016 Certifications to that date.

4. The January 3, 2017 Supplemental Notice and January 27, 2017 Letter

In anticipation of the January 31 deadline, the government updated the Court on these querying issues in the January 3, 2017 Notice. That Notice indicated that the IG's follow-on study (covering the first quarter of 2016) was still ongoing. A separate OCO review, limited in many of the same ways as the IG studies, and covering the periods of April through December 2015 and April through July of 2016, found that some [REDACTED] improper queries were conducted by [REDACTED] analysts during those periods.²¹ The January 3, 2017 Notice stated that "human error was the primary factor" in these incidents, but also suggested that system design issues contributed. For

²¹ NSA further reported that OCO reviewed queries involving a number of identifiers for known U.S. persons who were not targets under Sections 704 or 705(b) of the Act, and which were associated with "certain terrorism-related events that had occurred in the United States." January 3, 2017 Notice at 6. NSA OCO found [REDACTED] such queries, [REDACTED] of which improperly ran against Section 702 upstream Internet data. [REDACTED] of the improper queries were run in a system called [REDACTED] which NSA analysts use to [REDACTED] [REDACTED] of a current or prospective target of NSA collection, including under Section 702. *Id.* at 6-7.

~~TOP SECRET//SI//ORCON/NOFORN~~

Page 20

~~TOP SECRET//SI//ORCON/NOFORN~~

example, some systems that are used to query multiple datasets simultaneously required analysts to “opt-out” of querying Section 702 upstream Internet data rather than requiring an affirmative “opt-in,” which, in the Court’s view, would have been more conducive to compliance. See January 3, 2017 Notice at 5-6. It also appeared that NSA had not yet fully assessed the scope of the problem: the IG and OCO reviews “did not include systems through which queries are conducted of upstream data but that do not interface with NSA’s query audit system.” Id. at 3 n.6. Although NSD and ODNI undertook to work with NSA to identify other tools and systems in which NSA analysts were able to query upstream data, id., and the government proposed training and technical measures, it was clear to the Court that the issue was not yet fully scoped out.

On January 27, 2017, the government provided further information on the technical and training measures NSA was taking and proposed to take to address this issue. NSA was implementing its technical measures only on systems with respect to the system thought to be used most frequently to query Section 702 data. The government still had not ascertained the full range of systems that might have been used to conduct improper U.S.-person queries. See, e.g., January 27, 2017 Letter at 5 (“NSA is progressing with its efforts to identify other tools or systems that analysts are using to query upstream data.”). The government also reported that the NSA IG study for the first quarter of 2016 had found [REDACTED] improper queries, a substantial

~~TOP SECRET//SI//ORCON/NOFORN~~

Page 21

JA2811

~~TOP SECRET//SI//ORCON/NOFORN~~

improvement over the first quarter of 2015.²² But NSA was still working to determine the scope of its U.S.-person query problem and to identify all relevant storage systems and querying tools.

The January 27, 2017 Letter concluded that, “[b]ased on the complexity of the issues, NSA will not be in a position to provide thorough responses [to the Court’s questions] on or before January 31, 2017.” January 27, 2017 Letter. The government represented that a further extension of the Court’s time to consider the 2016 Certifications through May 26, 2017, would be consistent with the national security and would allow the government time to investigate and remedy the problem.

The Court granted an extension only through April 28, 2017.²³ January 27, 2017 Order at 6. In doing so, the Court noted its concern about the extent of non-compliance with “important safeguards for interests protected by the Fourth Amendment.” *Id.* at 5. The Court also observed that, while recent remedial measures appeared promising, they were being implemented only on certain systems, while other systems remained to be assessed. *Id.* at 5-6.

On March 17, 2017, the government reported that NSA was still attempting to identify all systems that store upstream data and all tools used to query such data, though that effort was nearly complete. March 17, 2017 Compliance Report at 100. NSA had also redoubled training on querying requirements and made technical upgrades to certain commonly-used querying tools

²² In addition to the findings of the IG and OCO reviews, the government identifies improper queries in the course of regular oversight efforts. The government reports those incidents to the Court through individual notices and quarterly reports.

²³ By operation of Section 1881a(i)(1)(B), the government’s submission on March 30, 2017, of amendments to the 2016 Certifications and revised procedures started a new 30-day period for Court review, which ends on April 29, 2017.

~~TOP SECRET//SI//ORCON/NOFORN~~

Page 22

~~TOP SECRET//SI//ORCON//NOFORN~~

that were designed to reduce the likelihood of non-compliant queries. *Id.* at 100-101.

Meanwhile, the government continued to report further compliance issues regarding the handling and querying of upstream Internet collection²⁴ and to investigate potential root causes of non-compliant querying practices. April 7, 2017 Preliminary Notice (Queries) at 4 n.4.

5. The 2017 Amendments

As embodied in the March 30, 2017 Submission, the government has chosen a new course: [REDACTED]; sequestering and then destroying raw upstream Internet data previously collected; and substantially narrowing the scope of upstream collection [REDACTED]. Most significantly, the government will eliminate “abouts” collection altogether, which will have the effect of eliminating acquisition of the more problematic types of MCTs. These changes should substantially reduce the acquisition of non-pertinent information concerning U.S. persons pursuant to Section 702.

As of March 17, 2017, NSA had [REDACTED]

[REDACTED]. Revisions to the NSA Minimization Procedures now state that all Internet transactions acquired on or before that date and existing in NSA’s institutionally managed

²⁴ See April 7, 2017, Preliminary Notice of Compliance Incidents Regarding the Labeling and Querying of Section 702-Acquired Data (“April 7, 2017 Preliminary Notice (Mislabeling)”) (nearly [REDACTED] communications acquired through upstream Internet collection were “incorrectly labeled” as acquired from Internet service providers and, as a result, likely subject to prohibited queries using U.S.-person identifiers); April 7, 2017, Preliminary Notice of Potential Compliance Incidents Regarding Improper Queries (“April 7, 2017 Preliminary Notice (Queries)”) (identifying another [REDACTED] potential violations of prohibition on using U.S.-person identifiers to query Internet upstream collection).

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 23

JA2813

~~TOP SECRET//SI//ORCON//NOFORN~~

repositories²⁵ will be sequestered pending destruction such that “NSA personnel will not be able to access the[m] for analytical purposes.” March 30, 2017 Memorandum at 4; see NSA Minimization Procedures §3(b)(4)a.

NSA will destroy such sequestered Internet transactions as soon as practicable through an accelerated age-off process. See NSA Minimization Procedures §3(b)(4)a. The government represents that the age-off may take up to one year to complete and verify (with quarterly reports to the Court), and that:

- Pending destruction, sequestered transactions (a) will not be subject to separate age-off or purge processes that otherwise would apply to them, see March 30, 2017 Memorandum at 15-16 & nn. 16-17; and (b) will be available only to NSA technical and compliance personnel for the limited purposes of ensuring the integrity of the systems used to store them and the controls that limit other employees’ access to them, see id. at 14 n.13; NSA Minimization Procedures §3(b)(4)a.
- Copies of sequestered transactions will remain in backup and archive systems, not available for use by intelligence analysts, until they age off of those systems in the ordinary course. See March 30, 2017 Memorandum at 14 n.13;
- Sequestered transactions may be retained for litigation purposes as contemplated by Section 3(c)(3) of the NSA Minimization Procedures, subject to prompt notification to the Court. See id. at 16-17 & n.18.
- Certain records derived from upstream Internet communications (many of which have been evaluated and found to meet retention standards) will be retained by NSA, even though the underlying raw Internet transactions from which they are

²⁵ The March 30, 2017 Submission does not define what an “institutionally managed repository” is. If the government intends not to apply the above-described sequester-and-destroy process to any information acquired on or before March 17, 2017, by Internet upstream collection because the information is not contained in an “institutionally managed repository,” it shall describe the relevant circumstances in a written submission to be made no later than June 2, 2017; however, the government need not submit such a description for circumstances referenced in this Opinion and Order as ones in which NSA may retain such information.

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 24

~~TOP SECRET//SI//ORCON/NOFORN~~

derived might be subject to destruction. These records include serialized intelligence reports and evaluated and minimized traffic disseminations; completed transcripts and transcriptions of Internet transactions; [REDACTED]; [REDACTED];²⁶ information used to support Section 702 taskings and FISA applications to this Court; and [REDACTED].²⁷ See March 30, 2017 Memorandum at 20-24.

Finally, upstream collection of Internet transactions [REDACTED]

[REDACTED] for communications to or from a targeted person, but “abouts” communications may no longer be acquired. The NSA Targeting Procedures are amended to state that “[a]cquisitions conducted under these procedures will be limited to communications *to or from* persons targeted in accordance with these procedures,” NSA Targeting Procedures § I, at 2 (emphasis added), and NSA’s Minimization Procedures now state that Internet transactions acquired after March 17, 2017, “that are not to or from a person targeted in accordance with NSA’s section 702 targeting procedures are unauthorized acquisitions and therefore will be destroyed upon recognition.” NSA Minimization Procedures § 3(b)(4)b.²⁸ Because they are regarded as unauthorized, the government will report any acquisition of such communications to the Court as an incident of non-compliance. See March 30, 2017 Memorandum at 17-18.

²⁶ [REDACTED]

See NSA Targeting Procedures § I at 6.

²⁷ [REDACTED]

[REDACTED] March 30, 2017 Memorandum at 23.

²⁸ The targeting procedures still require NSA either to use Internet Protocol (IP) filtering of upstream Internet collection to “limit such acquisitions to Internet transactions that originate and/or terminate outside the United States” or [REDACTED].
[REDACTED] Id.

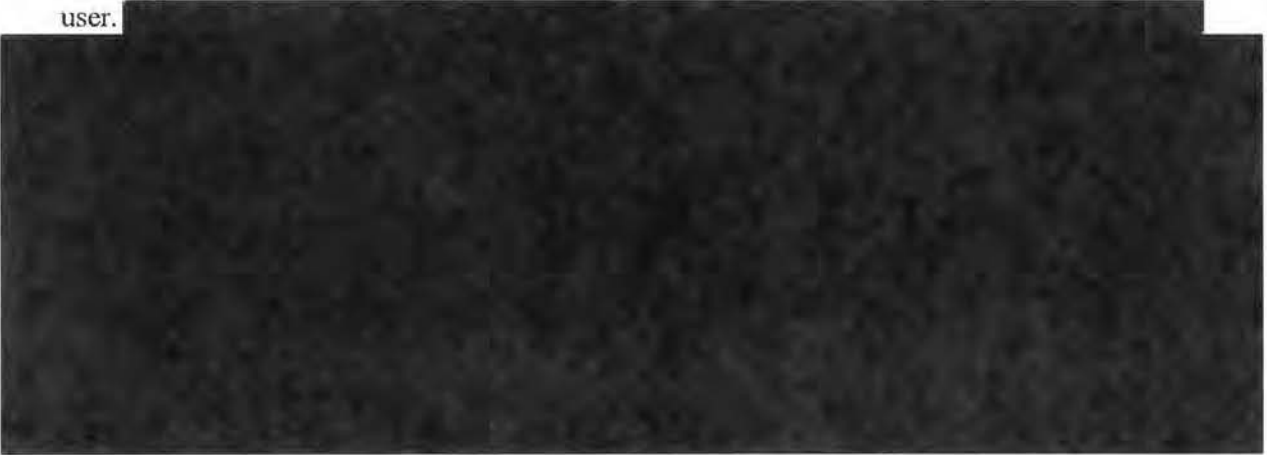
~~TOP SECRET//SI//ORCON/NOFORN~~

Page 25

~~TOP SECRET//SI//ORCON//NOFORN~~

Conforming changes are made throughout the NSA Minimization Procedures to remove references to “abouts” collection. Section 3(b)(4) of those procedures, in particular, is significantly revised and streamlined to reflect the narrower scope of authorized collection. For example, detailed procedures previously appearing in Section 3(b)(4) requiring sequestration and special handling of MCTs in especially problematic categories (e.g., those in which the “active user” is a non-target who is in the United States or whose location is unknown) are removed. Because NSA is no longer authorized to acquire those forms of MCTs, if it somehow acquires one, NSA must now destroy it upon recognition.²⁹

NSA may continue to acquire MCTs under the amended procedures, but only when it can ensure that the target is a party to the entire MCT or, in other words, when the target is the active user.



²⁹ Internet transactions properly acquired through NSA upstream collection after March 17, 2017, will continue to remain subject to a two-year retention limit, “unless the NSA specifically determines that at least one discrete communication within the Internet transaction meets the retention standards” in the NSA Minimization Procedures. See NSA Minimization Procedures § 3(c)(2). This reflects no change from the current procedures.

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 26

JA2816

~~TOP SECRET//SI//ORCON/NOFORN~~

[REDACTED]³⁰ See March 30, 2017

Memorandum at 10.

It will still be possible, however, for NSA to acquire an MCT that contains a domestic communication. For example, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] If NSA determines that the sender and all intended recipients of a discrete communication within an MCT were located in the United States at the time of that discrete communication, then the entire MCT must be promptly destroyed, see NSA Minimization Procedures § 5, unless the Director makes the required waiver determination for each and every domestic communication contained in the MCT. March 30, 2017 Memorandum at 9 n.9.³¹

U.S.-Person Queries. In light of the elimination of “abouts” communications from Section 702 upstream collection, the government proposes a change to Section 3(b)(5) of the NSA Minimization Procedures that would remove the prohibition on NSA analysts conducting

³⁰ This enumeration is without prejudice to NSA’s ability to acquire other types of communications if it can limit acquisition to communications to or from a target as required by the new procedures.

³¹ The NSA Minimization Procedures generally take an “all-or-nothing” approach to retention or destruction of MCTs. Thus, an MCT in which *any* discrete communication is not to or from a target is also subject to destruction in its entirety. See NSA Minimization Procedures § 3(b)(4)b; March 30, 2017 Memorandum at 13 n.12 (“[I]f for some reason NSA acquires an Internet transaction in which any discrete communication contained therein is not to or from a section 702 target, NSA must destroy such transactions upon recognition.”).

~~TOP SECRET//SI//ORCON/NOFORN~~

Page 27

~~TOP SECRET//SI//ORCON//NOFORN~~

queries of Internet upstream data using identifiers of known U.S. persons. Under this proposal, NSA analysts could query upstream data using known U.S. person identifiers, subject to the same requirements that apply to their queries of other Section 702-acquired data. Specifically, any query involving a U.S.-person identifier is subject to NSA internal approval requirements and “require[s] a statement of facts establishing that the use of any such identifier as a selection term is reasonably likely to return foreign intelligence information.” NSA is required to maintain records of all such determinations and those records are subject to review by NSD and ODNI. See NSA Minimization Procedures § 3(b)(5).³²

The Court agrees that the removal of “abouts” communications eliminates the types of communications presenting the Court the greatest level of constitutional and statutory concern. As discussed above, the October 3, 2011 Memorandum Opinion (finding the then-proposed NSA Minimization Procedures deficient in their handling of some types of MCTs) noted that MCTs in which the target was the active user, and therefore a party to all of the discrete communications within the MCT, did not present the same statutory and constitutional concerns as other MCTs. The Court is therefore satisfied that queries using U.S.-person identifiers may now be permitted to run against information obtained by the above-described, more limited form of upstream Internet collection, subject to the same restrictions as apply to querying other forms of Section

³² The Court understands that DOJ and ODNI review all U.S.-person identifiers approved for use in querying contents of Section 702-acquired communications as well as the written documentation of the foreign intelligence justifications for each such query during bi-monthly compliance reviews. See November 6, 2015 Opinion at 25 n.22.

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 28

JA2818

~~TOP SECRET//SI//ORCON/NOFORN~~

702-acquired data.³³ See generally October 3, 2011 Memorandum Opinion at 22-24 (finding that addition of a provision allowing NSA to query non-upstream Internet transactions using U.S. person identifiers was consistent with the statute and the Fourth Amendment); November 6, 2015 Opinion at 24-26 (after inviting views of amicus curiae on this issue, finding that the CIA and NSA minimization procedures permitting such queries comported with the statute and the Fourth Amendment).

The Court concludes that, taken as a whole, these changes strengthen the basis for finding that the NSA Targeting Procedures meet the requirements of Section 1881a(d)(1) and that the NSA Minimization Procedures meet the definition of such procedures in Section 1801(h). The elimination of “abouts” collection and, consequently, the more problematic forms of MCTs, focuses Section 702 acquisitions more sharply on communications to or from Section 702 targets, who are reasonably believed to be non-U.S. persons outside the United States and expected to receive or communicate foreign intelligence information. That sharper focus should have the effect that U.S. person information acquired under Section 702 will come more

³³ Of course, NSA still needs to take all reasonable and necessary steps to investigate and close out the compliance incidents described in the October 26, 2016 Notice and subsequent submissions relating to the improper use of U.S.-person identifiers to query terms in NSA upstream data. The Court is approving on a going-forward basis, subject to the above-mentioned requirements, use of U.S.-person identifiers to query the results of a narrower form of Internet upstream collection. That approval, and the reasoning that supports it, by no means suggest that the Court approves or excuses violations that occurred under the prior procedures.

~~TOP SECRET//SI//ORCON/NOFORN~~

Page 29

~~TOP SECRET//SI//ORCON//NOFORN~~

predominantly from non-domestic communications that are relevant to the foreign intelligence needs on which the pertinent targeting decisions were based.³⁴

D. NCTC Raw Take Sharing

1. Sharing of Unminimized Information Acquired Under [REDACTED] with NCTC

The September 26, 2016 Submission proposes for the first time to allow NCTC access to unminimized information acquired by NSA and FBI pursuant to [REDACTED]

[REDACTED] Previously, NCTC only had access to minimized Section 702-acquired information residing in FBI's general indices and relating to certain categories of investigations concerning international terrorism. NCTC has not, and will not under the government's proposal, engage in FISA collection of its own. It does, however, have significant experience with handling FISA-acquired information, including unminimized information obtained pursuant to Titles I and III and Sections 704 and 705(b) of the Act, pursuant to AG- and FISC-approved minimization procedures.

Beginning in 2008, NCTC was authorized to receive certain FISA-derived information from terrorism cases that FBI had uploaded into its Automated Case Support ("ACS") system. FISA information residing in ACS has been minimized by FBI and appears in investigative

³⁴ When the Court approved the prior, broader form of upstream collection in 2011, it did so partly in reliance on the government's assertion that, due to [REDACTED] some communications of foreign intelligence interest could only be acquired by such means. See October 3, 2011 Memorandum Opinion at 31 & n. 27, 43, 57-58. This Opinion and Order does not question the propriety of acquiring "abouts" communications and MCTs as approved by the Court since 2011, subject to the rigorous safeguards imposed on such acquisitions. The concerns raised in the current matters stem from NSA's failure to adhere fully to those safeguards.

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 30

~~TOP SECRET//SI//ORCON//NOFORN~~

reports and other work product. The FISC in 2008 found that NCTC's access to such information in ACS was "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information" under 50 U.S.C. § 1801(h)(1). Docket No. [REDACTED], Memorandum Opinion and Order entered on Oct. 8, 2008, at 3-6. Later, in 2012, NCTC was granted access to raw information from terrorism cases obtained under Titles I and III and Sections 704 and 705(b) of the Act, subject to expanded minimization procedures. See Docket Nos. [REDACTED], Memorandum Opinion and Order entered on May 18, 2012 ("May 18, 2012 Opinion").

NCTC also has experience handling information obtained under Section 702 of the Act. Since 2012, NCTC has had access to minimized information obtained under Section 702 through its access to certain case categories in FBI's general indices (including ACS and another system known as Sentinel). See Docket Nos. [REDACTED], Memorandum Opinion entered on Sept. 20, 2012, at 22-25 ("September 20, 2012 Opinion").

In each instance in which the FISC has authorized expanded sharing of FISA-acquired information with NCTC, the FISC has recognized NCTC's role as the government's primary organization for analyzing and integrating all intelligence pertaining to international terrorism and counterterrorism. For example, in approving NCTC's access to minimized Section 702-acquired information in FBI general indices in 2012, the FISC observed that NCTC was statutorily charged with ensuring that intelligence agencies receive all-source intelligence support and that executive and legislative branch officials have access to international terrorism-related intelligence information and analysis to meet their constitutional responsibilities. See id. at 23

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 31

~~TOP SECRET//SI//ORCON/NOFORN~~

(citing then-applicable statutory provisions); see also Affidavits of Nicholas Rasmussen, Director, NCTC, appended at Tab 5 to each of the 2016 Certifications, at 1. The government further avers in support of the current proposal that: (1) NCTC is statutorily charged with providing “strategic operational plans for the civilian and military counterterrorism intelligence and operations across agency boundaries, both inside and outside the United States;” and (2) the NCTC Director “is assigned ‘primary responsibility within the United States Government for conducting net assessments of terrorist threats.’” September 26, 2016 Memorandum at 12-13 (citing 50 U.S.C. § 3056(f)(1)(B) and (G)).

The Court is satisfied that NCTC’s receipt of information acquired under [REDACTED] [REDACTED] is consistent with its mission. As for the NCTC’s need to have access to this information in raw form, the government asserts that NCTC’s ability to obtain Section 702-acquired information more quickly and in a form closer to its original, and to examine that information in NCTC systems, using its own analytical tools in the context of potentially related information available in NCTC systems, will enhance NCTC’s ability to produce counterterrorism foreign intelligence information. See September 26, 2016 Memorandum at 13-14. The government provides an example in which NCTC was able to use its access to raw FISA-acquired information from collection under other provisions of FISA to provide a timely and unique assessment that was shared with other elements of the Intelligence Community in support of their intelligence collection and analysis functions. See id. at 15. One would hope that this is one of many such examples.

~~TOP SECRET//SI//ORCON/NOFORN~~

Page 32

JA2822

~~TOP SECRET//SI//ORCON//NOFORN~~

In any event, as noted above, the government's proffered rationale for sharing raw information with NCTC was accepted by the FISC in the context of information obtained under other provisions of the Act, and the Court is persuaded that it applies with equal force in the context of collection under Section 702. Among other things, the volume of collection under Section 702 militates in favor of bringing all available analytical resources to bear on the careful analysis and exploitation of foreign intelligence information from such collection. The Court also credits the assertion that time can be of the essence in many rapidly-unfolding counterterrorism investigations. The Court is persuaded that timely access to raw Section 702-acquired information will enhance NCTC's ability to perform its distinct mission, to support the activities of other elements of the Intelligence Community, and to provide valuable input to senior decisionmakers in the Executive Branch and Congress.

Moreover, the information acquired under [REDACTED] though voluminous – is the result of targeting persons reasonably believed to be non-United States persons located outside the United States. For that reason, it is unlikely to contain as high a proportion of information concerning United States persons as information acquired by FISA electronic surveillance and physical search, which often involve targets who are United States persons and typically are directed at persons in the United States.

To be sure, information concerning unconsenting United States persons has been and will continue to be acquired under Section 702 and [REDACTED] particularly. The minimization procedures must carefully regulate the government's use and dissemination of such U.S. person information in order to satisfy the definition of "minimization

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 33

JA2823

~~TOP SECRET//SI//ORCON//NOFORN~~

procedures” at Section 1801(h). The procedures NCTC will be required to follow with respect to its handling of such information are examined in detail below.

The Court also finds that the scope of the proposed sharing with NCTC is appropriate. Consistent with NCTC’s mission, the proposed sharing of unminimized Section 702-acquired information is limited to [REDACTED]. The government notes that the sharing will not include telephony data or the results of upstream Internet collection; in other words, it will be limited to Internet communications obtained with the assistance of the direct providers of the communication services involved. See September 26, 2016 Memorandum at 10-11. NCTC will receive raw information [REDACTED] and subject to the same limitations as CIA (no upstream Internet collection and no telephony).

Id.

The government undertakes to notify the Court before altering these arrangements and providing raw telephony or upstream Internet data to NCTC, FBI or CIA. See id. at 11 n.7; accord March 30, 2017 Memorandum at 9-10 n.10. With regard to upstream Internet collection, the Court has determined that mere notification to the FISC would be insufficient, especially as NSA is in the process of transitioning to a narrower form of collection and segregating and destroying the results of the prior, broader collection. Accordingly, the Court is ordering that raw information obtained by NSA’s upstream Internet collection under Section 702 shall not be provided to FBI, CIA or NCTC unless it is done pursuant to revised minimization procedures that are adopted by the AG and DNI and submitted to the FISC for review in conformance with Section 702.

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 34

~~TOP SECRET//SI//ORCON//NOFORN~~

With that limitation, the Court finds that NCTC's receipt of raw information acquired under [REDACTED] subject to appropriate minimization procedures as described below, will "minimize the . . . 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." 50 U.S.C. § 1801(h)(1).³⁵ The NCTC has followed AG- and FISC-approved minimization procedures in connection with its prior receipt of FISA-acquired information, including Section 702-acquired information, with relatively few documented instances of noncompliance. See generally Docket Nos. [REDACTED], Memorandum Opinion and Order entered on Aug. 26, 2014 Opinion ("August 26, 2014 Opinion") at 37 (noting that "no significant compliance issues have arisen under [NCTC's Section 702 minimization] procedures").

a. Changes to FBI and NSA Procedures Relating to Raw Information Sharing with NCTC

As noted above, the extension of raw information sharing to NCTC requires changes to several sets of procedures.³⁶ First, FBI's targeting procedures, and FBI and NSA's minimization procedures, are each amended to reflect the fact that those agencies may now provide to NCTC

³⁵ With regard to § 1801(h)(2)'s limitation on the dissemination of United States person identities, the Court adopts the analysis set out at pages 7-8 of the May 18, 2012 Opinion.

³⁶ Some technical, conforming edits to the certifications and procedures occasioned by the extension of raw information sharing to NCTC are not discussed herein because they raise no issues material to the Court's review. Certain other changes to the proposed certifications and procedures are not discussed for the same reason.

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 35

~~TOP SECRET//SI//ORCON//NOFORN~~

unminimized communications obtained under [REDACTED] See FBI Targeting Procedures § I.6; NSA Minimization Procedures § 6(c)(3); FBI Minimization Procedures § V.E. NCTC is required to identify to NSA those individual Section 702 selectors for which it wishes to receive unminimized information, and is required to apply its own approved minimization procedures to such information. See NSA Minimization Procedures § 6(c)(3); FBI Minimization Procedures § V.E.

b. Changes to NCTC Minimization Procedures Relating to Raw Information Sharing with NCTC

The NCTC Minimization Procedures have been enhanced significantly to account for its receiving raw information under Section 702. But they are not crafted out of whole cloth. They are modeled on the previously-approved minimization procedures that apply to NCTC's receipt of information under Titles I and III and Sections 704 and 705(b) of the Act.³⁷ Modifications are proposed to address issues that are unique to Section 702 collection and in some instances to harmonize the proposed NCTC procedures with those used by the FBI, NSA, and CIA in their handling of Section 702-acquired information. Several key elements of the NCTC Minimization Procedures are discussed below, focusing on instances in which they depart from the previously approved NCTC Title I Procedures.³⁸

³⁷ For ease of reference, this opinion refers to these procedures (the "National Counterterrorism Center Standard Minimization Procedures for Information Acquired by the Federal Bureau of Investigation Pursuant to Title I, Title III, or Section 704 or 705(b) of the Foreign Intelligence Surveillance Act") as the "NCTC Title I Procedures."

³⁸ The government does not propose targeting procedures for NCTC, so NCTC will not be authorized to engage in any Section 702 collection.

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 36

~~TOP SECRET//SI//ORCON//NOFORN~~

The NCTC Minimization Procedures do not have a provision restricting NCTC's processing, retention, and dissemination of third-party information. In NCTC's Title I Procedures, third-party information is defined to include "communications of individuals who are not the targets of the collection," and to exclude "any information contained in a communication to which the target is a party." NCTC Title I Procedures § A.3.h. Third-party information thus defined is subject to stricter retention, processing, and dissemination limitations under NCTC's Title I Procedures than information directly involving the target. *See id.* § C.4. In 2012, the FBI removed similar third-party information provisions from its Section 702 minimization procedures. In approving that change, the Court explained that in the context of Section 702 collection such rules

have no practical effect because the term "target" is defined as "the user(s) of a targeted selector." In light of that definition . . . there are no "third party" communications [in Section 702 collection] for the FBI to minimize. Because the deletion of the provisions regarding third party communications does not alter the manner in which the FBI acquires, retains, or disseminates Section 702 information, this change is not problematic under Section 1801(h).

September 20, 2012 Opinion at 17-18 (internal citations omitted). For the same reason, the omission of provisions present in NCTC's Title I Procedures governing the NCTC's retention, processing, and dissemination of third-party information from its Section 702 minimization procedures presents no impediment to their approval.

Exclusion and Departure Provisions. The NCTC Minimization Procedures contain certain exclusions and departure provisions that are consistent with the NCTC Title I Procedures with two notable exceptions:

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 37

JA2827

~~TOP SECRET//SI//ORCON//NOFORN~~

- (1) An exclusion is added for the performance of lawful oversight functions of NSD, ODNI, relevant Inspectors General, and NCTC itself, which is consistent with parallel provisions in other agencies' procedures. See NCTC Minimization Procedures § A.6.e; NSA Minimization Procedures § 1; FBI Minimization Procedures § I.G; CIA Minimization Procedures § 6(f); and
- (2) A separate exclusion addresses compliance with congressional and judicial mandates. NCTC Minimization Procedures § A.6.d.

The latter provision was amended across all the agencies' minimization procedures in the September 26, 2016 Submission and is the subject of separate discussion below.

U.S. Person Presumptions. In general, the procedures provide a rebuttable presumption that persons known to be in the United States are United States persons, and those known or reasonably believed to be outside the United States are non-United States persons. Id. § A.4.a and b. The NCTC Minimization Procedures diverge slightly from their Title I counterpart with respect to individuals whose locations are not known. [REDACTED]

[REDACTED] NCTC Title I Procedures § A.4.a. That approach makes sense in those procedures, which apply to information predominantly obtained by electronic surveillance and physical search – [REDACTED]

[REDACTED] – directed at persons in the United States. [REDACTED]

[REDACTED] Id. §

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

A.4.c. [REDACTED]

[REDACTED]

[REDACTED] NCTC Minimization Procedures

§A.4.e.

The Court assesses that Section 702 collection is more analogous to [REDACTED] than it is to other forms of collection that are regulated by the NCTC Title I Procedures and that the application of the [REDACTED] is appropriate in this context. Section 702 collection focuses exclusively on electronic data and communications collected with the assistance of electronic communication service providers, and its targets are reasonably believed to be non-U.S. persons located overseas. The presumption of non-U.S. person status for a communicant whose location is not known is also consistent with the presumptions allowed under the FBI and NSA's current and proposed Section 702 minimization procedures. See NSA Minimization Procedures § 2(k)(2); FBI Minimization Procedures § I.D. The Court finds the same framework reasonable as applied to NCTC's handling of Section 702 information and consistent with the requirements of Section 1801(h). See September 20, 2012 Opinion at 15-16 (approving parallel change to FBI Section 702 Minimization Procedures).³⁹

Retention. The NCTC Minimization Procedures impose a retention schedule and framework that are consistent with those followed by FBI for Section 702-acquired information

³⁹ The NCTC Minimization Procedures also include provisions regarding unincorporated associations and aliens who have been admitted for lawful permanent residence (NCTC Minimization Procedures § A.4.c and d) that track current provisions in the NSA Minimization Procedures (§ 2(k)(3) and (4)). The Court sees no issue with these provisions.

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 39

~~TOP SECRET//SI//ORCON/NOFORN~~

and, with a few immaterial exceptions not warranting separate discussion, with corresponding provisions of the NCTC Title I Procedures. In brief, information that the NCTC retains on an electronic and data storage system, but has not reviewed, generally must be destroyed after five years from the expiration date of the certification authorizing the collection. NCTC Minimization Procedures § B.2.a. Information retained on such systems that has been reviewed, but not identified as information that reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime is generally subject to special access controls after ten years from such expiration date, and shall be destroyed after fifteen years from such date. *Id.* § B.2.b.⁴⁰

In one respect, the proposed NCTC Minimization Procedures are more restrictive than the NCTC Title I Procedures: Unlike the NCTC Title I Procedures, the NCTC Minimization Procedures expressly provide that the prescribed time limits for retention apply to metadata repositories, NCTC Minimization Procedures § C.3; *see* October 4, 2016 Transcript at 7. They further require appropriate training and access controls for NCTC employees granted access to Section 702-acquired information. NCTC Minimization Procedures §§ B.1, F.1, F.2 and F.3. They also require that such information be maintained in secure systems that enable NCTC to mark or otherwise identify communications that meet the standards for retention. *Id.* Consistent with the procedures followed by other agencies, the NCTC Minimization Procedures require

⁴⁰ Generally speaking, information identified as meeting one of those criteria is not subject to the above-described temporal limitations on retention. *Id.* § B.3. *See*, however, the discussion on page 46 below regarding limitations on retention and use of evidence of a crime that is not foreign intelligence information.

~~TOP SECRET//SI//ORCON/NOFORN~~

Page 40

~~TOP SECRET//SI//ORCON//NOFORN~~

destruction of information obtained under a reasonable, but mistaken, belief that the target was appropriate for Section 702 collection, subject to limited waiver provisions. Id. § B.4. Finally, they include provisions for retention of information reasonably believed to be necessary for, or potentially discoverable in, administrative, civil or criminal litigation. Id. § B.5. Analogous provisions already appear in NSA's and CIA's Minimization Procedures. See NSA Minimization Procedures § 3(c)(4); CIA Minimization Procedures § 11.

Processing. The NCTC Minimization Procedures set standards for queries of data obtained under Section 702, including requiring written justifications for queries using U.S. person identifiers that are subject to subsequent review and oversight by NSD and ODNI. NCTC Minimization Procedures § C.1; see also id. § C.3 (metadata queries "must be reasonably likely to return foreign intelligence information"). They apply heightened handling requirements to sensitive information and privileged communications. The provisions for sensitive information are essentially identical to those found in the NCTC Title I Procedures. Compare NCTC Minimization Procedures § C.4 with NCTC Title I Procedures § C.5.

The proposed procedures for NCTC's handling of privileged communications obtained under Section 702 closely track those found in NSA's and CIA's Section 702 minimization procedures. Compare NCTC Minimization Procedures § C.5 with NSA Minimization Procedures § 4; CIA Minimization Procedures § 7. The NCTC Minimization Procedures require, among other things, the destruction of attorney-client communications that are affirmatively determined not to contain foreign intelligence information or evidence of a crime. See NCTC Minimization Procedures § C.5.a. If an attorney-client communication appears to contain foreign

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 41

~~TOP SECRET//SI//ORCON//NOFORN~~

intelligence information or evidence of a crime, [REDACTED]

[REDACTED] See *id.* § C.5.b, c, and e. Communications containing privileged information will be segregated when such information pertains to a criminal charge in the United States, [REDACTED]

[REDACTED] See *id.* § C.5.c, d, e, and f. [REDACTED]

[REDACTED] See *id.* § C.5.i. [REDACTED]

[REDACTED] See *id.* § C.5.g and h.

The Court closely examined substantial revisions to the NSA and CIA procedures as they relate to privileged communications in 2015, and found that they “serve to enhance the protection of privileged information” and “present no concern under Section 1801(h).” See November 6, 2015 Opinion at 18. The Court now finds the same to be true with respect to the NCTC Minimization Procedures.

Dissemination. The dissemination provisions of the NCTC Minimization Procedures (§ D) provide for disseminations in a manner consistent with CIA’s and NSA’s handling of Section 702-acquired information. They also track in all material respects the NCTC Title I Procedures, which have been found to satisfy Section 1801(h).

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

Handling of Information in FBI General Indices. The NCTC Minimization Procedures, like the NCTC Title I Procedures, include a separate section that addresses NCTC's handling of minimized Section 702 information made available to it through FBI's general indices. This provision of the NCTC Minimization Procedures tracks the corresponding provision of the NCTC Title I Procedures. Compare NCTC Minimization Procedures § E with NCTC Title I Procedures § E. The government points out that the description of individuals who are expected to be allowed access to information in such systems ("NCTC personnel") is meant to be broader than the defined term "NCTC employees" that is used in all other instances throughout the proposed NCTC Minimization Procedures. The government explains that the broader term "NCTC personnel" is meant to encompass (in addition to the NCTC employees, detailees, and contractors who would qualify as "NCTC employees" as defined in the proposed procedures, see NCTC Minimization Procedures § A.3.b) NCTC assignees from other agencies. The government explains that, consistent with the current NCTC Section 702 minimization procedures, such assignees will continue to have access to minimized information in FBI general indices but will not be allowed to access raw Section 702-acquired information. September 26, 2016 Memorandum at 15 n.9. The Court assesses that is a sensible distinction.

Two Additional Issues. Two particular provisions in the agencies' proposed minimization procedures relating to NCTC represent departures from current practice under Section 702 and merit separate discussion. Those provisions pertain to NCTC's retention of evidence of a crime and receipt of information from FBI and NSA for collection avoidance purposes.

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 43

JA2833

~~TOP SECRET//SI//ORCON//NOFORN~~

NCTC's Retention of Evidence of Crime. The predecessor procedures that regulated NCTC's retention, use, and dissemination of minimized Section 702 information obtained through FBI's general indices acknowledged that some of the information made available to NCTC might constitute evidence of a crime, but not foreign intelligence information or information necessary to understand such information or assess its importance. As a law enforcement agency, FBI would have a reason to maintain such information in its general indices, where NCTC employees might encounter it. NCTC, as a non-law-enforcement agency, was precluded under its previous Section 702 minimization procedures from retaining (in its own systems), using or disseminating such information. By contrast, under the new NCTC Minimization Procedures (and only with respect to information it receives in raw form),⁴¹ NCTC may retain and disseminate evidence of a crime for law enforcement purposes. *See* NCTC Minimization Procedures §§ A.7, D.2. This proposed approach is consistent with Sections A.7 and D.2 of the NCTC Title I Procedures.

The government asserts that, under the proposed NCTC Minimization Procedures, NCTC might review raw information that has not been, and may never be, reviewed by any other agency. As such, the government posits, NCTC must disseminate evidence of a crime to meet its "crime reporting obligations" under Executive Order 12333 and other applicable law. See

⁴¹ As noted above, the new NCTC Minimization Procedures incorporate (in Section E) the rules currently governing NCTC's retention, use, and dissemination of minimized information that it obtains through FBI's general indices. NCTC continues to be prohibited from retaining, using or disseminating information it obtains from those indices that constitutes evidence of a crime, but not foreign intelligence information, with anyone, including law enforcement, for reasons explained below. See NCTC Minimization Procedures § E.2

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 44

~~TOP SECRET//SI//ORCON//NOFORN~~

September 26, 2016 Memorandum at 16-17. Under NCTC's minimization procedures as now in effect, NCTC only has access to information from FBI indices that has already been reviewed and minimized by FBI, so it is presumed that FBI would have taken all necessary steps with respect to actionable law enforcement information. Under that construct, NCTC could, as required by its procedures, simply disregard and delete that information from its holdings (unless there was a foreign intelligence reason for NCTC to retain it). The government asserts that the same would not be true with respect to raw information passed to NCTC. See id.

It is less readily apparent, however, why NCTC would need to retain evidence of a crime after it has been passed to a law enforcement agency. The government asserts that NCTC needs to preserve original copies of the relevant information in order to be able to respond to potential follow-on requests for information or assistance from law enforcement. See October 4, 2016 Transcript at 4-6.⁴² In other words, NCTC would have no reason to retain the information for its own purposes, but it would have a need for retention that derives from the needs of the law enforcement agency to which NCTC passed the information. The government further posits that NCTC may be the only agency that retains a copy of the relevant information and thus may be the only entity able to respond to follow-up requests from law enforcement. See October 4, 2016 Transcript at 5.

⁴² The government correctly points out that in its opinion approving the NCTC's Title I Procedures, which contain identical provisions with respect to crime reporting and evidence of a crime, the Court found that those provisions met the statutory definition of minimization procedures in Section 1801(h)(3), which prescribes procedures that "allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes." See September 26, 2016 Memorandum at 16 n.10.

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 45

~~TOP SECRET//SI//ORCON//NOFORN~~

The Court credits the government's explanation of NCTC's derivative need to retain such information for law enforcement purposes. It bears emphasis, however, that NCTC may retain and disseminate evidence of a crime that is not foreign intelligence information or necessary to understand foreign intelligence information or assess its importance and otherwise would be subject to destruction under the generally applicable age-off schedule, see NCTC Minimization Procedures § B.2, only in furtherance of those law enforcement purposes. See id. § D.2. The Court understands and expects that NCTC will only retain such information – including after it has been disseminated in compliance with crime reporting obligations, see id. § A.7 – for so long as is reasonably necessary to respond to law enforcement requests of the kind posited by the government. In the interim, NCTC shall make no independent use of such information. The Court directs the government to take steps to ensure that NCTC abides by these limitations and that any failures to do so are appropriately identified and reported to the FISC.

Collection Avoidance. The FBI and NSA would also be allowed, under proposed amendments to their respective procedures, to share with NCTC for “collection avoidance” purposes information about domestic communications obtained under Section 702 that indicate that a targeted person is in the United States or otherwise should no longer be targeted under Section 702. See NSA Minimization Procedures § 5; FBI Minimization Procedures § III.A. These provisions now allow sharing of such information among FBI, NSA, and CIA. At first it was not clear to the Court why this provision should be extended to include NCTC, given that NCTC engages in no independent collection under Section 702, or, so far as the Court is aware, under any other authorities. [REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 46

JA2836

~~TOP SECRET//SI//ORCON//NOFORN~~

██ Indeed, it seemed counterintuitive to the Court that an agency not engaged in collection would need to receive information, otherwise subject to destruction, for “collection avoidance purposes.”

The government’s response is that NCTC, upon receipt of such information, might be in a position to “connect the dots” and identify other individuals who might not be viable targets for Section 702 collection (or perhaps other facilities that might be used by the same individual and should not be targeted). See September 26, 2016 Memorandum at 17-18. Such information would also put NCTC on notice that the selector, or related selectors, might not be viable for nomination to be targeted for collection by other agencies. Id. The government adds that FBI and NSA typically only share the minimum information necessary for collection avoidance purposes, such as technical information from the relevant communication or a mere notification that the communication triggered a flag regarding the propriety of targeting someone. Id.

Because the government offers a plausible explanation of the need for sharing such information with NCTC, the Court is prepared to approve the provisions in question, with the understanding that NCTC may not use or disclose this information except as needed for collection avoidance purposes.⁴³

Subject to the above-described understandings, the Court finds that the proposed minimization procedures for NCTC’s handling of raw information acquired under ██████████

⁴³ NSA’s procedures, for example, require that a domestic communication retained for collection avoidance purposes be placed on the NSA’s “Master Purge List” (“MPL”), which prevents further analytical use or dissemination of the communication for any other reason. See NSA Minimization Procedures § 5.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

██████████ and the modifications to the other agencies' procedures relating to NCTC's receipt of such information, are reasonable. The NCTC Minimization Procedures address retention, use, and dissemination of Section 702-acquired information in ways that are consistent with logical analogues. Indeed, the FISC has approved all the major elements of those procedures in the context of other FISA minimization procedures, and the Court finds that, taken as a whole and as applied to raw information acquired under ██████████ ██████████, the NCTC Minimization Procedures conform to 50 U.S.C. § 1801(h).

E. Other Changes to Targeting and Minimization Procedures in the September 26, 2016 Submission

1. Changes to FBI Minimization Procedures Permitting the Retention of Section 702-Acquired Information Subject to Preservation Obligations Arising from Litigation

In 2014, the FISC approved provisions permitting FBI, NSA, and CIA to retain Section 702-acquired information subject to specific preservation obligations arising in litigation concerning the lawfulness of Section 702. See August 26, 2014 Opinion at 21-25. Under those provisions, information otherwise subject to destruction under the agencies' respective minimization procedures would nonetheless be retained to satisfy litigation preservation obligations. Access to information retained under those provisions is tightly restricted. See id. at 21, 23.

The NSA and CIA minimization procedures accompanying the 2015 Certifications included revisions to these "litigation hold" provisions. Among other things, those procedures included new provisions whereby NSA and CIA may retain for litigation purposes Section 702-

~~TOP SECRET//SI//ORCON/NOFORN~~

Page 48

~~TOP SECRET//SI//ORCON//NOFORN~~

acquired information otherwise subject to destruction requirements that are not set forth in the minimization procedures, provided that access to such information is strictly controlled as prescribed in the procedures.⁴⁴ The government must promptly notify the Court and seek its approval whenever this provision is invoked. See NSA Minimization Procedures § 3(c)(4)b; CIA Minimization Procedures § 11.b.

The litigation hold provisions also require NSA and CIA to provide DOJ with a summary of all litigation matters requiring preservation of Section 702-acquired information, a description of the Section 702-acquired information being retained, and, if possible based on the information available to the agencies, the status of each litigation matter. See NSA Minimization Procedures § 3(c)(4)a and b; CIA Minimization Procedures § 11.a and b.⁴⁵ The FISC, in considering the 2015 Certifications, appointed amicus curiae to help it evaluate these litigation hold provisions. The FISC agreed with the amicus's assessment that the revised litigation hold provisions "comport with the requirements of Section 1801(h) and strike a reasonable and appropriate

⁴⁴ As stated in the November 6, 2015 Opinion, the Court understands this provision to apply to destruction requirements arising under a FISC order, a FISC rule, or other FISC-approved procedures – e.g., the requirement that NSA destroy any communication acquired through the intentional targeting of a person reasonably believed to be a United States person or to be located in the United States, see NSA Targeting Procedures § IV.

⁴⁵ The FISC has ordered the government to submit a report at the end of each year identifying matters in which FBI, NSA or CIA is retaining Section 702-acquired information that would otherwise be subject to destruction in order to satisfy a litigation preservation obligation. See August 26, 2014 Opinion at 42. The Court has reviewed the litigation hold reports filed by the government in December 2015 and December 2016. The Court is reaffirming that reporting obligation and extending it to NCTC.

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 49

~~TOP SECRET//SI//ORCON/NOFORN~~

balance between the retention limitations reflected in FISA and the government's need to comply with its litigation-related obligations." November 6, 2015 Opinion at 16.

The proposed NCTC Minimization Procedures, like NSA's and CIA's, include litigation hold provisions that address departures from destruction requirements arising under NCTC's minimization procedures and from other sources. See NCTC Minimization Procedures § B.5.

The government proposes now to expand the FBI Minimization Procedures to address the latter situation and to bring FBI's litigation hold provisions more closely into line with those of the other agencies. [REDACTED]

[REDACTED]

[REDACTED]


[REDACTED] In 2015, with the concurrence of a FISC-appointed amicus curiae, the FISC found these procedures appropriate as applied to NSA and CIA. November 6, 2015 Opinion at 16. The Court sees no basis for a contrary conclusion now with regard to the NCTC and FBI.

The Court emphasizes, however, the need promptly to notify and seek leave of the Court to retain information pursuant to such provisions. [REDACTED]

[REDACTED]

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~



at 2-3. The Court will not look favorably on similarly lengthy delays in deciding whether to comply with an otherwise applicable destruction requirement or seek FISC approval to retain information in anticipation of bringing criminal charges.

2. Clarification of Age-off Requirements for Encrypted Information Under the FBI Minimization Procedures

In its 2015 Submission, the government added a new provision to the FBI Minimization Procedures permitting the FBI to retain Section 702-acquired information that is encrypted or believed to contain secret meaning for any period of time during which such material is subject to, or of use in, cryptanalysis or otherwise deciphering secret meaning. Access to such information is restricted to FBI personnel engaged in cryptanalysis or deciphering secret meaning. See FBI Minimization Procedures § III.G.5. Nonpublicly available information concerning unconsenting United States persons retained under the provision cannot be used for any other purpose unless such use is permitted under a different provision of the minimization procedures. See id. Once information retained under this provision is decrypted or its secret meaning is ascertained, the generally-applicable retention rules apply. The government stated that it would calculate the age-off date for such information from the later of the date of decryption or the date of expiration of the certification pursuant to which the information was

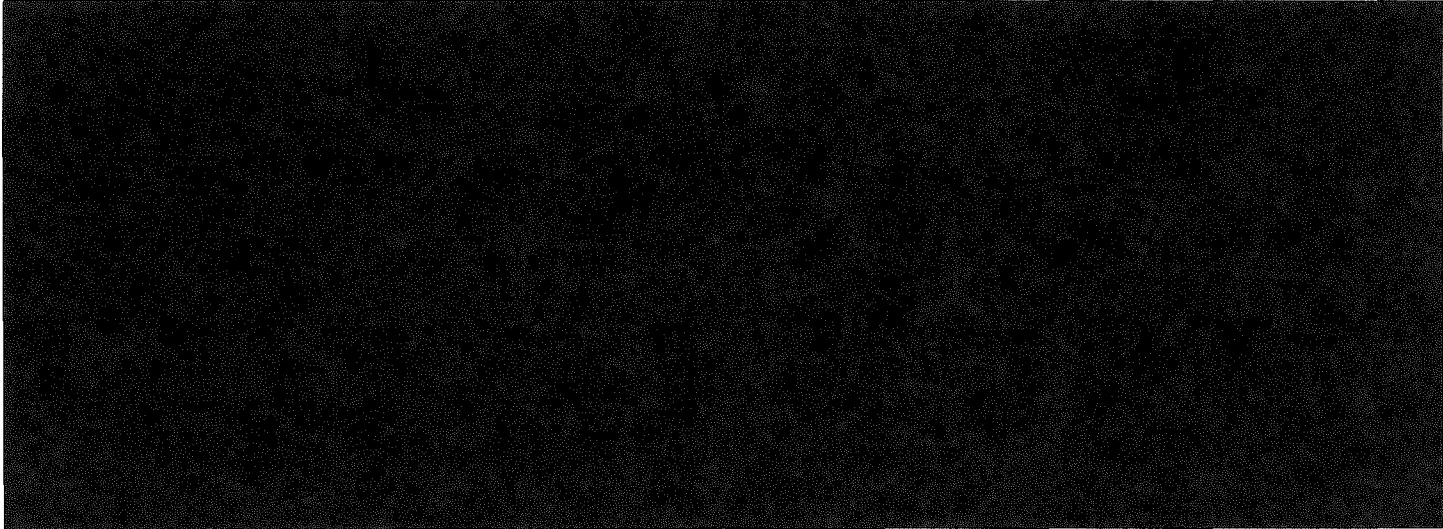
~~TOP SECRET//SI//ORCON//NOFORN~~

Page 51

~~TOP SECRET//SI//ORCON//NOFORN~~

acquired. See Docket Nos. [REDACTED] July 15, 2015, Memorandum Regarding 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 at 18. But the procedures themselves were silent on this point.

When it approved the 2015 Certifications, the FISC encouraged the government to make this calculation methodology explicit in future versions of the procedures. November 6, 2015 Opinion at 20 n.19. The government has done so. The FBI Minimization Procedures now



3. Revisions to Minimization Provisions Permitting Compliance with Judicial or Legislative Mandates

The NSA and CIA minimization procedures approved in the November 6, 2015 Opinion each state that “[n]othing in these procedures shall prohibit the retention, processing, or dissemination of information reasonably necessary to comply with specific constitutional, judicial, or legislative mandates.” See November 6, 2015 Opinion at 21 (citing relevant provisions of procedures). The FISC took issue with the facial breadth of these provisions,

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 52

~~TOP SECRET//SI//ORCON//NOFORN~~

observing that “[a] provision that would allow the NSA and CIA to deviate from any of the[] restrictions [in their respective minimization procedures] based upon unspecified ‘mandates’ could undermine the Court’s ability to find that the procedures satisfy” statutory requirements. Id. at 22. The FISC addressed this issue in three ways. First, in order to avoid finding a deficiency in the procedures, it applied an interpretive gloss that the government had previously articulated with regard to similar language in another set of minimization procedures, to the effect that such provisions would be invoked sparingly and applied only to directives specifically calling for the information at issue, and not to Executive Branch orders or directives. Id. at 22. The FISC emphasized that it “must construe the phrase ‘specific constitutional, judicial, or legislative mandates’ to include only those mandates containing language that clearly and specifically requires action in contravention of an otherwise-applicable provision of the requirement of the minimization procedures.” Id. at 23. Second, to ensure that these provisions were actually applied in a manner consistent with the FISC’s understanding, the government was directed to report any action in reliance on this provision to the FISC promptly and in writing, along with a written justification for each such action. Id. at 23-24.⁴⁶ Finally, the government was encouraged to consider replacing these broadly-worded provisions with language more narrowly tailored to the above-described intent. Id. at 24 n.20.

The government proffered revisions to these provisions in the September 26, 2016 Submission. The provisions, as revised and incorporated in all of the agencies’ minimization

⁴⁶ This reporting requirement is carried forward by this Opinion and Order. The Court understands that this provision has not yet been invoked.

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 53

~~TOP SECRET//SI//ORCON/NOFORN~~

procedures, now require that the departure be “necessary to comply with a specific congressional mandate or order of a court within the United States.” NSA Minimization Procedures § 1; FBI Minimization Procedures § I.G; CIA Minimization Procedures § 6.g; NCTC Minimization Procedures § A.6.d. The Court finds the revised language acceptable, but again wishes to emphasize that it expects this provision to be interpreted narrowly.

As described in the September 26, 2016 Memorandum at 6-7, the government has received requests from members of Congress, including 14 members of the House Judiciary Committee, for estimates of the number of communications of U.S. persons that have been acquired under Section 702. Responding to such requests would require NSA, and possibly other agencies, to structure queries designed to elicit information concerning U.S. persons with no foreign intelligence purpose, facially in violation of applicable minimization procedures. Such requests, which have not taken the form of a subpoena or other legal process, would not constitute legal mandates for purposes of the departure provision discussed above. Instead, the government submits that, in order to respond to such requests, it may take actions that contravene otherwise applicable minimization requirements pursuant to provisions of the minimization procedures that allow for performance of lawful oversight functions. For example, the NSA Minimization Procedures state that nothing in them shall restrict “NSA’s performance of lawful oversight functions of its personnel or systems, or lawful oversight functions” of NSD, ODNI, or relevant Inspectors General. NSA Minimization Procedures § 1; see also FBI Minimization Procedures § I.G (same); CIA Minimization Procedures § 6.f (same); NCTC Minimization Procedures § A.6.e (same). The government also undertook to notify the Court

~~TOP SECRET//SI//ORCON/NOFORN~~


Page 54


~~TOP SECRET//SI//ORCON/NOFORN~~

“promptly” if it “uses this provision to respond to such congressional oversight inquiries.”

September 26, 2016 Memorandum at 7.⁴⁷

Although these provisions could more clearly address responses to requests from congressional overseers, the Court believes they can be fairly read to authorize actions necessary to respond to the requests described by the government. The Court directs the government to provide prompt written notification of any instance when an agency acts in contravention of otherwise applicable minimization requirements in order to respond to an oversight request from any outside entity other than those currently specified in its procedures. The Court expects the government to make such a submission regarding its response to the above-referenced congressional requests promptly upon completion of that response.

4. Amendment of FBI Targeting Procedures with Respect to 



⁴⁷ The government has since orally notified the Court that, in order to respond to these requests and in reliance on this provision of its minimization procedures, NSA has made some otherwise-noncompliant queries of data acquired under Section 702 by means other than upstream Internet collection.

~~TOP SECRET//SI//ORCON/NOFORN~~

Page 55

~~TOP SECRET//SI//ORCON/NOFORN~~



The Court does not view this change, which deals with [REDACTED]

[REDACTED] agencies authorized to receive unminimized Section 702-acquired information, as problematic, provided that information is shared only with entities authorized to receive it (in the case of NCTC, information obtained pursuant to [REDACTED]). The legality of raw information sharing fundamentally rests on the foreign intelligence need to provide the information to the receiving agency and that agency's implementation of FISA-compliant minimization procedures.

Accordingly, the Court concludes that this change does not preclude it from finding that the FBI Targeting Procedures meet the requirements of Section 1881a(d)(1).

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

F. Conclusions

1. The NSA and FBI Targeting Procedures Comply With Statutory Requirements and Are Reasonably Designed to Prevent the Targeting of United States Persons

To summarize, the proposed changes to NSA's targeting procedures now make clear that acquisitions thereunder will be limited to communications to or from persons targeted for

acquisition under Section 702. FBI's revised targeting procedures allow it to [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] The Court has no difficulty finding that these changes, individually and taken together, do not detract from its earlier holdings with regard to the sufficiency and legality of the FBI and NSA targeting procedures.

For the reasons stated above and in the Court's opinions in the Prior 702 Dockets, the Court concludes that the NSA Targeting Procedures and the FBI Targeting Procedures, as written, are reasonably designed, as required by Section 1881a(d)(1): (1) to ensure that any acquisition authorized under the 2016 Certifications is limited to targeting persons reasonably believed to be located outside the United States, and (2) 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. Moreover, for the reasons stated above and in the Court's opinions in the Prior 702 Dockets, the Court concludes that the NSA and FBI Targeting Procedures, as written, are reasonably designed to prevent United States persons from

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 57

~~TOP SECRET//SI//ORCON//NOFORN~~

being targeted for acquisition – a finding that is relevant to the Court’s analysis, which is set out below, of whether the procedures are consistent with the requirements of the Fourth Amendment.

2. The FBI, NSA, CIA, and NCTC Minimization Procedures Comply With Statutory Requirements

For the reasons stated above and in the Court’s opinions in the Prior 702 Dockets, the Court similarly concludes that the NSA, FBI, CIA, and NCTC Minimization Procedures satisfy the definition of minimization procedures at Section 1801(h). In the November 6, 2015 Opinion, the FISC found that the minimization procedures accompanying the 2015 Certifications met statutory and constitutional standards. The FISC recommended two changes to the procedures in future submissions. In both instances, the government has acted on those suggestions, proposing changes to narrow the “legal mandate” exception to each agency’s minimization procedures and define more precisely the time limits placed on FBI’s retention of information believed to be encrypted or contain secret meaning. Both changes further cabin the relevant agencies’ discretion and enhance the protection of nonpublicly available information concerning unconsenting United States persons.⁴⁸

Other changes to minimization procedures pertain to FBI’s retention of information for “litigation hold” purposes and enable sharing [REDACTED] [REDACTED] with NCTC. (As noted above, NCTC’s revised procedures incorporate

⁴⁸ As discussed above, the NSA Minimization Procedures have been revised to eliminate acquisition of “abouts” communications and the most problematic forms of MCTs. As a result of that change, the Court no longer views the prohibition on U.S.-person queries in NSA upstream collection to be necessary to comport with the statute or, as discussed below, the Fourth Amendment.

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 58

~~TOP SECRET//SI//ORCON//NOFORN~~

elements from various other procedures, with appropriate adaptations to fit the context of Section 702.) The Court concludes that none of the proposed changes to the agencies' minimization procedures, individually or collectively, precludes the Court from finding that such procedures comport with Section 1801(h).

Accordingly, the Court finds that the agencies' proposed minimization procedures meet the requirements of 50 U.S.C. § 1801(h). That finding is made in reliance on (1) the above-stated limitations on (a) the types of information that will, and will not, be shared in raw form with the FBI, CIA, and NCTC, and (b) NCTC's retention, use or disclosure of evidence of a crime and information received from other agencies for collection avoidance purposes; and (2) the expectation that the government will faithfully comply with the reporting requirements set forth below, in the procedures themselves, and in Rule 13 of the FISC Rules of Procedure.

G. The Targeting and Minimization Procedures Are Consistent with the Fourth Amendment

The Court must also assess whether the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment. See 50 U.S.C. § 1881a(i)(3)(A).

The Fourth Amendment 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.

U.S. Const. amend. IV.

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 59

~~TOP SECRET//SI//ORCON//NOFORN~~

Reasonableness is “the ultimate touchstone of the Fourth Amendment.” In re Certified Question of Law, Docket No. 16-01, Opinion at 31 (FISA Ct. Rev. Apr. 14, 2016) (per curiam) (“In re Certified Question”)⁴⁹ (quoting Riley v. California, 134 S. Ct. 2473, 2482 (2014)).⁵⁰ In assessing the reasonableness of a governmental intrusion under the Fourth Amendment, a court must “balance the interests at stake” under the “totality of the circumstances.” In re Directives at 20. Specifically, a court must “balance . . . the degree of the government’s intrusion on individual privacy” against “the degree to which that intrusion furthers the government’s legitimate interest.” In re Certified Question at 31. “The more important the government’s interest, the greater the intrusion that may be constitutionally tolerated.” In re Directives at 19-20.

If the protections that are in place for individual privacy interests are sufficient in light of the governmental interest at stake, the constitutional scales will tilt in

⁴⁹ A declassified version of this opinion is available at: www.dni.gov/files/icotr/FISCR%Opinion%2016-01.pdf.

⁵⁰ Although “[t]he warrant requirement is generally a tolerable proxy for ‘reasonableness’ when the government is seeking to unearth evidence of criminal wrongdoing, . . . it fails properly to balance the interests at stake” when “the government is instead seeking to preserve the nation’s security from foreign threats.” In re Certified Question at 3. Accordingly, a warrant is not required to conduct surveillance “to obtain foreign intelligence for national security purposes . . . directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States.” In re Directives Pursuant to Section 105B of FISA, Docket No. 08-01, Opinion at 18-19 (FISA Ct. Rev. Aug. 22, 2008) (“In re Directives”). (A declassified version of In re Directives is available at 551 F.3d 1004 (FISA Ct. Rev. 2008)). The FISC has repeatedly reached the same conclusion regarding Section 702 acquisitions. See, e.g., November 6, 2015 Opinion at 36-37; September 4, 2008 Opinion at 34-36; accord United States v. Hasbajrami, 2016 WL 1029500 at *7-*9 (E.D.N.Y. March 8, 2016); United States v. Mohamud, 2014 WL 2866749 at *15-*18 (D. Or. June 24, 2014).

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 60

~~TOP SECRET//SI//ORCON/NOFORN~~

favor of upholding the government's actions. If, however, those protections are insufficient to alleviate the risks of government error and abuse, the scales will tip toward a finding of unconstitutionality.

Id. at 20.

“Collecting foreign intelligence with an eye toward safeguarding the nation’s security serves . . . a particularly intense interest” that is “different from the government’s interest in the workaday enforcement of the criminal law.” In re Certified Question at 29 (internal quotation marks omitted); see also id. at 31 (noting “the paramount interest in investigating possible threats to national security”). For that reason, “the government’s investigative interest in cases arising under FISA is at the highest level and weighs heavily in the constitutional balancing process.”

Id. at 32.

On the other side of the balance is the degree of intrusion on individual privacy interests protected by the Fourth Amendment. The degree of intrusion here is limited by restrictions on how the government targets acquisitions under Section 702 and how it handles information post-acquisition. For reasons explained above, the Court has found that the targeting procedures now before it are reasonably designed to limit acquisitions to targeted persons reasonably believed to be non-United States persons located outside the United States, whose privacy interests are not protected by the Fourth Amendment. See, e.g., November 6, 2015 Opinion at 38; September 4, 2008 Opinion at 37 (citing United States v. Verdugo-Urquidez, 494 U.S. 259, 274-75 (1990)). That is not to say, however, that targeting non-United States persons located outside the United States for acquisition under Section 702 never implicates interests protected by the Fourth Amendment. Under the revised procedures, the government may acquire communications to

~~TOP SECRET//SI//ORCON/NOFORN~~

Page 61

~~TOP SECRET//SI//ORCON/NOFORN~~

which United States persons and persons within the United States are parties when such persons communicate with a Section 702 target.⁵¹ Therefore it is necessary to consider how information from those communications will be handled.

Steps taken by the government to restrict the use or disclosure of information after it has been acquired can reduce the intrusiveness of the acquisition for purposes of assessing its reasonableness under the Fourth Amendment. See In re Certified Question at 35. In the Prior 702 Dockets, the FISC found that “earlier versions of the various agencies’ targeting and minimization procedures adequately protected the substantial Fourth Amendment interests that are implicated by the acquisition of communications of such United States persons.” November 6, 2015 Opinion at 38-39 (citing August 26, 2014 Opinion at 38-40; August 30, 2013 Opinion at 24-25). Specifically, “the combined effect of these procedures” was “to substantially reduce the risk that non-target information concerning United States persons or persons inside the United States will be used or disseminated’ and to ensure that ‘non-target information that is subject to protection under FISA or the Fourth Amendment is not retained any longer than is reasonably necessary.’” November 6, 2015 Opinion at 39 (quoting August 26, 2014 Opinion at 40).

The November 6, 2015 Opinion included a careful analysis of the rules for querying Section 702 information using United States person identifiers under the minimization procedures for the NSA, the CIA, and especially the FBI. See November 6, 2015 Opinion at 24-

⁵¹ NSA’s elimination of “abouts” collection should reduce the number of communications acquired under Section 702 to which a U.S. person or a person in the United States is a party.

~~TOP SECRET//SI//ORCON/NOFORN~~

Page 62

~~TOP SECRET//SI//ORCON//NOFORN~~

36, 39-45. After receiving briefing and oral argument from an amicus curiae appointed under 50 U.S.C. § 1803(i)(2)(B), the FISC concluded that, although its review did not involve treating each query as a separate action subject to a test for Fourth Amendment reasonableness, the querying rules were relevant to its assessment of whether the procedures as a whole were reasonable under the Fourth Amendment. November 6, 2015 Opinion at 40-41. The FISC further determined that the querying rules did not preclude a finding that the procedures were consistent with the requirements of the Fourth Amendment. *Id.* at 44-45.

In the procedures now before the Court, the relevant provisions of the CIA and FBI minimization procedures remain unchanged, *see* CIA Minimization Procedures at § 4; FBI Minimization Procedures at §§ III.D, IV.D, and the NCTC procedures generally track the pertinent requirements of the CIA Minimization Procedures. *See* NCTC Minimization Procedures at § C.3.⁵²

With regard to the querying rules in the CIA and NCTC procedures, the Court adopts the analysis of the November 6, 2015 Opinion.

As discussed above, NSA's procedures now limit all acquisitions – including upstream Internet acquisitions – to communications to or from an authorized Section 702 target. That limitation places upstream Internet collection in a posture similar to other forms of Section 702 collection for the purpose of assessing reasonableness under the Fourth Amendment. The revised procedures subject NSA's use of U.S. person identifiers to query the results of its newly-

⁵² Unlike the CIA procedures, the NCTC procedures require that queries of Section 702 metadata, as well as contents, be reasonably designed to return foreign intelligence information. NCTC Minimization Procedures at § C.3.

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 63

~~TOP SECRET//SI//ORCON/NOFORN~~

limited upstream Internet collection to the same limitations and requirements that apply to its use of such identifiers to query information acquired by other forms of Section 702 collection. See NSA Minimization Procedures § 3(b)(5). For that reason, the analysis in the November 6, 2015 Opinion remains valid regarding why NSA's procedures comport with Fourth Amendment standards of reasonableness with regard to such U.S. person queries, even as applied to queries of upstream Internet collection.

As discussed in the November 6, 2015 Opinion, the FBI's minimization procedures contemplate queries conducted to elicit foreign intelligence information and queries conducted to elicit evidence of crimes. With respect to the latter type of query, the FISC's approval of the FBI minimization procedures in 2015 was bolstered by the government's assessment that "FBI queries designed to elicit evidence of crimes unrelated to foreign intelligence rarely, if ever, produce responsive results" from Section 702 information. See November 6, 2015 Opinion at 44. To confirm the continued accuracy of that assessment, the FISC ordered the government to report on "each instance after December 4, 2015, in which FBI personnel receive and review Section 702-acquired information that the FBI identifies as concerning a United States person in response to a query that is not designed to find and extract foreign intelligence information." Id. at 78.

The government has reported one set of queries as responsive to this requirement. On [REDACTED], an FBI analyst reviewing Section 702 information found an email message in which a person in the United States gave detailed descriptions of violent, abusive acts [REDACTED] committed [REDACTED] children. [REDACTED] Notice regarding FBI queries of Section 702-

~~TOP SECRET//SI//ORCON/NOFORN~~

Page 64

~~TOP SECRET//SI//ORCON//NOFORN~~

acquired information designed to return evidence of a crime unrelated to foreign intelligence (“██████████ Notice”), at 2. In an effort to identify additional evidence of abuse, the FBI ran queries of Section 702 information using the names of the suspected abuser, the apparent victims, and other terms derived from that e-mail message. Those queries only retrieved the previously reviewed e-mail message from which the query terms were derived. Id. Pursuant to Section I.F of its minimization procedures, the FBI disseminated information about the child abuse to a local child protective services agency, ██████████
██████████ Id.

The undersigned judge finds persuasive the November 6, 2015 Opinion’s analysis of the FBI’s querying rules. The single reported instance of queries that returned U.S. person information unrelated to foreign intelligence information does not detract from that analysis, especially since those queries did not result in any further intrusion on privacy: they merely retrieved information already known to the analyst who ran the queries.⁵³

For the reasons stated above, neither the NCTC’s receipt of unminimized information acquired regarding counterterrorism targets, subject to its applying the NCTC Minimization Procedures, nor the other above-described modifications to the targeting and minimization procedures, causes the Court to deviate from prior assessments that the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment.

⁵³ The Court notes, however, that the FBI did not identify those queries as responsive to the Court’s reporting requirement until NSD asked whether any such queries had been made in the course of gathering information about the Section I.F dissemination. ██████████ Notice at 2. The Court is carrying forward this reporting requirement and expects the government to take further steps to ensure compliance with it.

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 65

~~TOP SECRET//SI//ORCON//NOFORN~~

IV. THE COMPLIANCE AND IMPLEMENTATION ISSUES REPORTED BY THE GOVERNMENT DO NOT WARRANT A FINDING THAT, AS IMPLEMENTED, THE TARGETING AND MINIMIZATION PROCEDURES ARE DEFICIENT.

The FISC has consistently understood its review of targeting and minimization procedures under Section 702 to include examining how the procedures have been and will be implemented. See, e.g., November 6, 2015 Opinion at 7; August 30, 2013 Opinion at 6-11, 19-22; April 7, 2009 Opinion at 22-25. As the Foreign Intelligence Surveillance Court of Review has noted, FISC “supervision of the execution of pen register orders further reduces the risk that such measures will be employed under circumstances, or in a manner, that unreasonably intrudes on individuals’ privacy interests.” In re Certified Question at 36-37. The same conclusion applies to FISC examination of how the government implements the Section 702 procedures.

For purposes of this examination, “the controlling norms are ones of reasonableness, not perfection,” November 6, 2015 Opinion at 45, under both Section 702⁵⁴ and the Fourth Amendment.⁵⁵ The Court evaluates the reasonableness of “the program as a whole,” not of individual actions in isolation. November 6, 2015 Opinion at 40-41. The assessment of

⁵⁴ See 50 U.S.C. § 1881a(d)(1) (requiring targeting procedures that are “reasonably designed to” limit targeting to “persons reasonably believed to be located outside the United States” and to “prevent the intentional acquisition” of communications to which all parties are known to be in the United States); § 1881a(e)(1) (requiring minimization procedures as defined in §§ 1801(h)(1) or 1821(4), i.e., procedures “reasonably designed” to minimize acquisition and retention, and to prohibit dissemination, of information concerning United States persons, consistent with foreign intelligence needs).

⁵⁵ See, e.g., United States v. Knights, 534 U.S. 112, 118 (2001) (“The touchstone of the Fourth Amendment is reasonableness”); In re Directives at 34 (surveillances found to be reasonable under the Fourth Amendment where “the risks of error and abuse are within acceptable limits and effective minimization procedures are in place”).

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 66

~~TOP SECRET//SI//ORCON//NOFORN~~

reasonableness takes due account of the fact that implementing Section 702 is “a large and complex endeavor . . . effected through thousands of discrete targeting decisions for individual selectors,”⁵⁶ each of which implicates selector-specific pre-tasking and post-tasking requirements, November 6, 2015 Opinion at 45-46, and that for all information acquired under Section 702, minimization procedures impose “detailed rules concerning . . . retention, use, and dissemination” *Id.* at 46. As the FISC has previously observed:

Given the number of decisions and volume of information involved, it should not be surprising that occasionally errors are made. Moreover, the government necessarily relies on ██████████ processes in performing post-tasking checks, *see, e.g.*, August 30, 2013 Opinion at 7-9, and in acquiring, routing, storing, and when appropriate purging Section 702 information. *See, e.g.*, April 7, 2009 Opinion at 17-22. Because of factors such as changes in communications technology or inadvertent error, these processes do not always function as intended.

Id.

Overall, the Court concludes that the targeting and minimization procedures satisfy applicable statutory requirements and are reasonable under the Fourth Amendment, despite the reported instances of non-compliance in prior implementation. The Court bases this conclusion in large measure on the extensive oversight conducted within the implementing agencies and by the DOJ and ODNI. Due to those efforts, it appears that compliance issues are generally

⁵⁶ For example, NSA “reports that, on average, approximately ██████████ facilities were under task at any given time between December 1, 2016 and February 28, 2017.” March 17, 2016 Compliance Report at 1 (footnote omitted). Facilities tasked for acquisition include ██████████

Id. at 1 n.1. “Additionally, between December 1, 2016 and February 28, 2017, the [FBI] reports that it received and processed approximately ██████████ *Id.* at 1.

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 67

~~TOP SECRET//SI//ORCON//NOFORN~~

identified and remedied in a timely and appropriate fashion.⁵⁷ Nonetheless, the Court believes it beneficial to discuss certain ongoing or recent compliance issues and, in some cases, direct the government to provide additional information.

A. Resolution of Issues Addressed in the November 6, 2015 Opinion

The November 6, 2015 Opinion discussed several significant compliance problems that were then pending. See November 6, 2015 Opinion at 47-77. With the exception of non-compliance with minimization procedures related to attorney-client privileged communications, which are discussed separately, those compliance issues have been resolved as described below.

1. Failure of Access Controls in FBI's [REDACTED]

[REDACTED] while the 2015 Certifications were pending, the government filed a notice (“[REDACTED] Notice”) indicating that a failure of access controls in an FBI database containing raw Section 702-acquired information resulted in [REDACTED] FBI employees improperly receiving access to such information. [REDACTED] Notice at 1. Specifically,

[REDACTED]

⁵⁷ Too often, however, the government fails to meet its obligation to provide prompt notification to the FISC when non-compliance is discovered. See FISC Rule of Procedure 13(b). For example, it is unpersuasive to attribute – even “in part” – an eleven-month delay in submitting a preliminary notice to “NSA’s efforts to develop remedial steps,” see April 7, 2017 Preliminary Notice (Mislabeling) at 1 n.1, 2, when the purpose of a preliminary notice is to advise the Court while investigation or remediation is still ongoing. See also, e.g., February 28, 2017 Notice of a Compliance Incident Regarding Incomplete Purges of Information Obtained Pursuant to Multiple FISA Authorities (“February 28, 2017 Notice”) at 1-2, n.3 (five-month delay attributed “to administrative issues surrounding the reorganization of NSA offices and personnel”). The Court intends to monitor closely the timeliness of the government’s reporting of non-compliance regarding Section 702 implementation.

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 68

~~TOP SECRET//SI//ORCON/NOFORN~~

[REDACTED] allowed [REDACTED] users access to Section 702-acquired information, *id.*, when only [REDACTED] were cleared for such access. *Id.* at 1, n.1. This resulted in violations of Sections III.A. and III.B of the FBI's minimization procedures.⁵⁸ The government provided testimony on this issue at a hearing on

[REDACTED] filed a Supplemental Notice on [REDACTED] indicating that [REDACTED] FISA-acquired products were "exported" [REDACTED] users who were not authorized to access these products. [REDACTED] Notice at 2.

On [REDACTED], the government filed what was styled as a Final Notice on this issue [REDACTED] Notice"). That notice indicated that the FBI [REDACTED] [REDACTED] had not disseminated the FISA-acquired products; and all [REDACTED] users had deleted from their systems the raw FISA-acquired information they had exported. [REDACTED]

⁵⁸ As then in effect and as now proposed, Section III.A of the FBI Minimization Procedures requires the FBI to "retain all FISA-acquired information under appropriately secure conditions that limit access to such information only to authorized users in accordance with [the FBI Minimization Procedures] and other applicable FBI procedures." FBI Minimization Procedures § III.A. Section III.B of the FBI Minimization Procedures further requires the FBI to grant access to raw Section 702-acquired information in a manner that is "consistent with the FBI's foreign intelligence information-gathering and information-sharing responsibilities, . . . [p]ermitting access . . . only by individuals who require access in order to perform their job duties[.]" *Id.* § III.B. It also requires users with access to FISA-acquired information to receive training on minimization requirements. *Id.* § III.B.4.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] In the Court's assessment, the government has appropriately remedied this incident.

2. NSA Failures to Complete Required Purges

On July 13, 2015, the Government filed a notice regarding NSA's purge processes for FISA-acquired information in its mission management systems ("July 13, 2015 Notice"). That notice indicated that the NSA had not been removing records associated with Section 702 data subject to purge from its [REDACTED] database. July 13, 2015 Notice at 3.

On October 5, 2015, the government filed a Supplemental Notice regarding NSA's purge processes for FISA-acquired information ("October 5, 2015 Notice"). That notice indicated that NSA had now removed from [REDACTED] all Section 702-acquired records that were marked as subject to purge. October 5, 2015 Notice at 2. On October 28, 2015, however, the government filed another Supplemental Notice regarding NSA's purge processes ("October 28, 2015 Notice") in which it reported that a technical malfunction in [REDACTED] had rendered the aforementioned purges incomplete. October 28, 2015 Notice at 2.

On January 14, 2016, the government filed a Supplemental Notice ("January 14, 2016 Notice") indicating that as of October 30, 2015, [REDACTED] was properly configured to remove records subject to purge and corresponding to identifiers on the MPL. January 14, 2016

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 70

~~TOP SECRET//SI//ORCON//NOFORN~~

Notice at 2. At that time NSA had completed purging records that had been added to the MPL between 2011 and 2015. *Id.* On September 22, 2016, the government filed another Supplemental Notice (“September 22, 2016 Notice on [REDACTED] confirming that as of February 2016, the NSA had removed from [REDACTED] all historical Section 702-acquired records subject to purge.”⁵⁹ September 22, 2016 Notice on [REDACTED] at 2.

The July 13, 2015 Notice also reported “a compliance incident regarding FISA-acquired information subject to purge or age off that [was] being retained in two of NSA’s compliance mission management systems, [REDACTED] and [REDACTED] in a manner that is “potentially inconsistent with NSA’s FISA-related minimization procedures.” July 13, 2015 Notice at 2, 5. Subsequent communications between the government and FISC staff revealed that [REDACTED] and [REDACTED] may also have been retaining data, the use or disclosure of which could violate 50 U.S.C. § 1809(a)(2). The November 6, 2015 Opinion directed the government to provide additional information about NSA’s retention of certain categories of information in [REDACTED] and [REDACTED] November 6, 2015 Opinion at 78.

On December 18, 2015, the government filed a detailed description of its plan and timeline for remedying improper retention in [REDACTED] and [REDACTED]. See Prior 702 Dockets, Verified Response to the Court’s Order Dated November 6, 2015, filed on Dec. 18,

⁵⁹ The government also disclosed in the January 14, 2016 Notice that [REDACTED] was not configured to age off all FISA-acquired information pursuant to relevant minimization procedures. January 14, 2016 Notice at 2. As of August 3, 2016, the NSA had removed from [REDACTED] all Section 702-acquired information identified as due for destruction under the retention periods set by the NSA Minimization Procedures, and prospectively, the NSA will remove Section 702-acquired information from [REDACTED] in compliance with those retention periods. September 22, 2016 Notice on [REDACTED] at 2.

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 71

~~TOP SECRET//SI//ORCON//NOFORN~~

2015. On September 22, 2016, the government provided a written update on the NSA's efforts to remove from [REDACTED] and [REDACTED] information that was subject to purge or age-off under the NSA Minimization Procedures ("September 22, 2016 Notice on [REDACTED] and [REDACTED] As of February 17, 2016, NSA had removed from [REDACTED] and [REDACTED] all Section 702-acquired information subject to age-off under the five- and two-year retention periods set by the NSA Minimization Procedures. September 22, 2016 Notice on [REDACTED] and [REDACTED] at 2. As of September 9, 2016, the NSA had deleted from [REDACTED] and [REDACTED] all historical Section 702-acquired data potentially subject to § 1809(a)(2), and it had developed a plan to deal prospectively with information potentially subject to § 1809(a)(2). *Id.* at 3. Finally, as of September 9, 2016, the NSA had removed from [REDACTED] and [REDACTED] other categories of information that the November 6, 2015 Opinion had identified as not permissible for retention in [REDACTED] and [REDACTED] (e.g., attorney-client communications that do not contain foreign intelligence information or evidence of a crime). *Id.* at 3-4.

B. Issues Arising Under the NSA Targeting Procedures

NSA's targeting procedures require that analysts, before tasking a selector for acquisition, make a reasonable assessment that the user of the selector is a non-U.S. person located outside the United States. See NSA Targeting Procedures § 1. Post-tasking, analysts are required to take reasonable steps to confirm that the selector continues to be used by a non-U.S. person located outside the United States. See NSA Targeting Procedures § 2. Those requirements directly bear on statutory limitations on Section 702 acquisitions. See 50 U.S.C. § 1881a(c)(1)(A), (d)(1)(A)

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 72

~~TOP SECRET//SI//ORCON/NOFORN~~

(targeting procedures must be reasonably designed to ensure that acquisitions are limited to targeting persons reasonably believed to be outside the United States); § 1881a(b)(3), (4) (government may not intentionally target a United States person reasonably believed to be outside the United States or intentionally acquire any communication as to which the sender and all intended recipients are known at time of acquisition to be in the United States).

Compliance and implementation issues have arisen regarding these pre-tasking assessments and post-tasking reviews. While those issues merit discussion, the Court does not believe they are sufficiently serious or pervasive to warrant finding that the targeting procedures do not meet the above-described statutory requirements or are inconsistent with the Fourth Amendment.

1. Scope of Pre-Tasking Review of [REDACTED]

One of the measures taken by NSA analysts to fulfill pre-tasking obligations is to check

[REDACTED] for information that may be probative of [REDACTED]

[REDACTED] For example, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED].

According to a notice filed by the government on August 24, 2016, NSA analysts often relied on the above-referenced [REDACTED] tool to [REDACTED] as part of those pre-tasking checks. August 24, 2016 Update Regarding the Scope of Section 702 Pre-Tasking Review of [REDACTED] at 2 (“August 24, 2016 Update”). The data returned [REDACTED] was

~~TOP SECRET//SI//ORCON/NOFORN~~

Page 73

~~TOP SECRET//SI//ORCON/NOFORN~~

limited, as [redacted] only [redacted]

[redacted]. Id. In certain circumstances, the results from [redacted] could have provided an incomplete and misleading impression of [redacted]

[redacted]. The government acknowledges that the sufficiency of running a [redacted] [redacted] as the sole basis for a pre-tasking assessment “depends upon the information known about the target from other sources and the nature of the information returned by the [redacted] [redacted]. Id. Subsequent investigation revealed [redacted] instances of improper taskings. See August 24, 2016 Update at 2, n.2. NSA placed on its MPL information obtained as a result of these taskings. Id. at 2.⁶⁰

NSA has developed a new tool for analysts to use for pre-tasking checks [redacted]
[redacted] August 24, 2016 Update at 4. “In addition to [redacted], NSA’s new tool is also [redacted] that will greatly enhance analysts’ pre-tasking reviews.” Id.

⁶⁰ For discussion of the government’s processes for purging Section 702 information, see March 17, 2017 Compliance Report at 2-5.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

While the described functionality of the new tool improves on some of the limitations of [REDACTED] it should not be seen as a panacea. In the Court's view, the fundamental cause of these improper taskings was not the limitations of [REDACTED] or other [REDACTED] tools, but rather the failure of analysts in these particular cases to pursue reasonable lines of inquiry regarding [REDACTED] [REDACTED]. See, e.g., August 24, 2016 Update at 3 [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]. It remains the obligation of analysts to exercise due diligence in the particular circumstances of each pre-tasking review, rather than to presume that using a given [REDACTED] tool or protocol will suffice. The government acknowledges that sometimes, after deploying the new tool, "additional research will be necessary to satisfy the totality of the circumstances test [for pre-tasking reviews] contained in the NSA Targeting Procedures," id. at 5, and addresses in its training efforts how NSA analysts should understand and comply with this requirement. See October 4, 2016 Transcript at 19-20.

2. Frequency of Post-Tasking Review of Contents

While the government did not report the following information as involving non-compliance with the NSA's targeting procedures, the Court believes it bears significantly on how those procedures are implemented and therefore merits discussion.

The NSA's targeting procedures do not require analysts to review the contents of communications acquired from tasking a particular selector at fixed intervals. Instead, they provide that such content review "will be conducted according to analytic and intelligence

~~TOP SECRET//SI//ORCON/NOFORN~~

Page 75

~~TOP SECRET//SI//ORCON//NOFORN~~

requirements and priorities.” See, e.g., NSA Targeting Procedures § II at 6.⁶¹ As previously described to the FISC, however, NSA follows a policy whereby such content review is performed no later than [REDACTED] days after the first acquisition and at intervals of no more than [REDACTED] days thereafter. See September 13, 2016, Update Regarding Post-Targeting Content Reviews (“September 13, 2016 Update”) at 2; Docket No. [REDACTED]

[REDACTED], Memorandum Opinion at 9-10 (FISA Ct. Oct. 24, 2014).

NSA and FBI analysts with access to Section 702 data are trained on this policy, while CIA analysts receive training that “is consistent with” the policy and are instructed “to review content as it is acquired.” September 13, 2016 Update at 3.⁶² According to a supplemental letter filed on March 13, 2017 (“March 13, 2017 Supp. Letter”), the government monitors compliance with the policy with regard to Section 702 data in an NSA repository called [REDACTED] but otherwise does not comprehensively monitor or verify whether analysts in fact conduct content reviews in conformance with that policy. March 13, 2017 Supp. Letter at 2.⁶³ For that reason,

⁶¹ This content review is in addition to other post-tasking steps to ascertain whether a tasked facility is being used inside the United States, such as [REDACTED]

[REDACTED] Id. § II at 6-7.

⁶² [REDACTED]

[REDACTED] See NSA Targeting Procedures § 2 at 7 n. 2-3.

⁶³ NSA routes most forms of Internet communications acquired under Section 702 to a repository called [REDACTED] March 13, 2017 Supp. Letter at 2. For review of communications in [REDACTED] NSA has [REDACTED] that monitors whether content checks are performed, sends prompts to analysts to conduct [REDACTED] and [REDACTED] reviews, and sends overdue notices. Id. at 1-2. NSA does not have such an alert system for other repositories containing

(continued...)

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 76

~~TOP SECRET//SI//ORCON//NOFORN~~

deviations from the policy may not be detected unless and until the circumstances are examined for other purposes. See September 13, 2016 Update at 3.

To address this concern, the government undertakes “to notify the Court . . . when, in connection with compliance incidents, the government also learns that content was not reviewed in accordance with the applicable policy.” Id. at 4. The government further undertakes to advise the FISC “of the total number of instances in which the government’s investigation into a potential [non-compliance] incident revealed that content review was not timely conducted in accordance with [this policy],” even if the government determines that, strictly speaking, there was no violation of the targeting procedures themselves. See id. That figure will be included in each of the government’s quarterly compliance reports. Id.

On March 13, 2017, the government reported the results of an examination of the performance of [REDACTED] and [REDACTED] content reviews for data in [REDACTED] during January-March 2016. March 13, 2017 Supp. Letter at 2. That examination revealed a compliance rate of approximately 79% for [REDACTED] reviews and 99% for [REDACTED] reviews. Id. NSA plans to issue an advisory to personnel reminding them of the policy. Id. at 3.

The Court intends to scrutinize the information submitted regarding future deviations from this policy. It also encourages the government to explore further measures, through

⁶³(...continued)

Section 702 information, though it has plans to develop systems for additional repositories by the end of 2017. Id. at 2-3. FBI and CIA do not have comparable systems. October 4, 2016 Transcript at 21, 24.

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 77

~~TOP SECRET//SI//ORCON//NOFORN~~

██████████ processes or otherwise, to prompt analysts to conduct content reviews in accordance with this policy, and to monitor or verify adherence to it.

C. Issues Arising Under the NSA Minimization Procedures

In addition to the improper use of U.S.-person identifiers to query the results of upstream Internet data discussed above, noteworthy compliance issues have arisen with regard to NSA's upstream collection of Internet communications and querying of Section 702-acquired data.

1. NSA Upstream Collection of Internet Communications

Under the pre-2017 Amendments version of the NSA Minimization Procedures, NSA is required to "take reasonable steps post-acquisition to identify and segregate through technical means" those MCTs that are particularly likely to involve communicants in the United States; specifically, those for which "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." NSA Minimization Procedures § 3(b)(4)a. (prior to the 2017 Amendments). Those procedures permit only certain 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" to access MCTs that have been segregated in the manner described above. § 3(b)(4)a.2. Information in a segregated MCT "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

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 78

JA2868

~~TOP SECRET//SI//ORCON/NOFORN~~

sender and all intended recipients are reasonably believed to be located in the United States.” § 3(b)(4)a.2.(a).⁶⁴

Starting in April 2015, a [REDACTED] error affected NSA’s upstream collection [REDACTED]. See September 30, 2016 Supplemental Notice of Compliance Incident Regarding Collection Pursuant to Section 702 (“September 30, 2016 Supp. Notice”) at 1. The error was discovered on January 26, 2016, and corrected on a going-forward basis the next day. Id.

This [REDACTED] error led to two types of compliance problems. First, it resulted in the unauthorized acquisition of Internet “communications from facilities that only partially matched authorized Section 702 [selectors] (e.g., [REDACTED])” Id. at 1-2. It appears that the government has taken appropriate steps to identify and purge the improperly acquired information. Id. at 2-3. NSA has positively identified [REDACTED] “data objects” as having been subject to this over-collection. Id. In addition, based on the nature of the [REDACTED] error and the technical characteristics of information likely to have been improperly collected due to the error, NSA has identified in excess of [REDACTED] “data objects” that may have been over-collected. Id. at 3. Because it was not technically feasible for NSA to identify within that set any and all objects that actually had been over-collected, NSA has put [REDACTED]-plus objects, as well as the [REDACTED] objects positively identified as having been over-collected, on its MPL. Id.; see also March 17, 2017 Quarterly Report at 114-15.

⁶⁴ In practice, however, no analysts received the requisite training in order to work with the segregated MCTs. October 4, 2016 Transcript at 41-43.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

Second, the [REDACTED] error resulted in failures in the technical processes whereby NSA identified MCTs that are subject to the segregation regime described above. Specifically, some MCTs may have been wrongly identified and labeled as ones in which the active user was the target, which would have resulted in those MCTs not being segregated. September 30, 2016 Supp. Notice at 3-4. To the extent wrongly-identified MCTs were actually ones for which the active user is reasonably believed to have been located in the United States or for whom the active user's location was unknown, they should have been segregated and subject to the above-described heightened access controls. Any large-scale failure to identify and segregate MCTs subject to those heightened access controls would have threatened to undermine one of the safeguards on which the FISC relied in 2011 when it approved the procedures adopted by the government in response to the FISC's prior finding of deficiency. See November 30, 2011 Opinion at 11-15.

The Court did not find entirely satisfactory the government's explanations of the scope of those segregation errors and the adequacy of its response to them and addressed some of its concerns at the October 4, 2016 Hearing. See, e.g., October 4, 2016 Transcript at 35-38.⁶⁵ Questions about the adequacy of steps previously taken to respond to the errors, however, are no longer material to the Court's review of the NSA Minimization Procedures. Under the revised

⁶⁵ The government later reported it had inadvertently misstated the percentage of NSA's overall upstream Internet collection during the relevant period that could have been affected by this [REDACTED] error (the government first reported the percentage as roughly 1.3%, when it was roughly 3.7%). April 11, 2017 Notice of Material Misstatement and Supplemental Notice of Compliance Incidents Regarding Collection Pursuant to Section 702 at 2.

~~TOP SECRET//SI//ORCON/NOFORN~~

Page 80

~~TOP SECRET//SI//ORCON//NOFORN~~

NSA Minimization Procedures, the results of upstream Internet collection during the relevant timeframe must be segregated and destroyed.

2. Improper Querying ██████ Communications

U.S. person identifiers may be used to query Section 702 data only if they are first “approved in accordance with [internal] NSA procedures, which must require a statement of facts establishing that the use of any such identifier as a selection term is reasonably likely to return foreign intelligence information.” NSA Minimization Procedures § 3(b)(5).⁶⁶ In performing such queries, NSA analysts sometimes use a tool called “█████ ██████” can be used to query data repositories, including one called ██████ September 30, 2016 Final Notice of Compliance Incidents Regarding Improper Queries (“September 30, 2016 Final Notice”) at 1. ██████ ██████ communications acquired pursuant to Section 702, as well as other FISA authorities. Id.

In May and June 2016, NSA reported to oversight personnel in the ODNI and DOJ that, since approximately 2012, use of ██████ to query communications in ██████ had resulted in inadvertent violations of the above-described querying rules for Section 702 information. Id. The violations resulted from analysts not recognizing the need to avoid querying datasets for which querying requirements were not satisfied or not understanding how to formulate ██████ queries to exclude such datasets. Id. at 1-2.

⁶⁶ As previously noted, NSA may not use U.S.-person identifiers to query the results of upstream Internet collection until the 2017 Amendments take effect, but will be able to run such queries of the narrower form of upstream Internet collection contemplated under the 2017 Amendments, subject to the approval process described above.

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 81

~~TOP SECRET//SI//ORCON//NOFORN~~

NSA examined all queries using identifiers for “U.S. persons targeted pursuant to Sections 704 and 705(b) of FISA using the [REDACTED] tool in [REDACTED] . . . from November 1, 2015 to May 1, 2016.” *Id.* at 2-3 (footnote omitted). Based on that examination, “NSA estimates that approximately eighty-five percent of those queries, representing [REDACTED] queries conducted by approximately [REDACTED] targeted offices, were not compliant with the applicable minimization procedures.” *Id.* at 3. Many of these non-compliant queries involved use of the same identifiers over different date ranges. *Id.* Even so, a non-compliance rate of 85% raises substantial questions about the propriety of using of [REDACTED] to query FISA data. While the government reports that it is unable to provide a reliable estimate of the number of non-compliant queries since 2012, *id.*, there is no apparent reason to believe the November 2015-April 2016 period coincided with an unusually high error rate.

The government reports that NSA “is unable to identify any reporting or other disseminations that may have been based on information returned by [these] non-compliant queries” because “NSA’s disseminations are sourced to specific objects,” not to the queries that may have presented those objects to the analyst. *Id.* at 6. Moreover, [REDACTED] query results are generally retained for just [REDACTED] *Id.*⁶⁷

The NSA has taken steps to educate analysts on the proper use of [REDACTED] it has provided a “reminder” to all analysts about the need “to limit queries across authorities in [REDACTED] with

⁶⁷ Information retrieved by an improper query might nonetheless satisfy the requirements for dissemination; indeed, absent a second violation of the minimization procedures, separate from the improper query, one would expect any disseminated information to have satisfied those requirements.

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 82

~~TOP SECRET//SI//ORCON//NOFORN~~

an explanation of how different types of queries operate; it issued a separate “Compliance Advisory,” which further addressed querying practices using ██████████ to all NSA target offices; and it revised a “banner” presented to users of ██████████ to emphasize that U.S. person identifiers should never be used for a type of query (called a “selector query”) that runs “against all data [that] an analyst is authorized to access.” *Id.* at 1, 6.

At the October 4, 2016 Hearing, the government represented that, based on ongoing oversight efforts, those measures appear to have been effective in improving how analysts use ██████████ to query Section 702 data. October 4, 2016 Transcript at 47-49. On April 3, 2017, the government reported to the Court that it had reaffirmed that assessment, based on discussions with NSA analysts and the absence of additional non-compliant queries using ██████████ April 3, 2017, Supplemental Notice of Compliance Incidents Regarding Improper Queries, at 3. In view of these remedial steps, the Court believes that, notwithstanding the above-described non-compliance, the NSA Minimization Procedures meet the statutory definition of “minimization procedures” and are consistent with the requirements of the Fourth Amendment.

D. Issues Arising Under the FBI Minimization Procedures

The following violations of the FBI’s minimization procedures merit discussion.

1. Improper Disclosures of Raw Information

On March 9, 2016, DOJ oversight personnel conducting a minimization review at the FBI’s ██████████ learned that the FBI had disclosed raw FISA information, including but not limited to Section 702-acquired information, to a ██████████ ██████████ ██████████ Compliance Report at 92. ██████████ is part of the ██████████

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

[REDACTED] and “is largely staffed by private contractors” [REDACTED]
[REDACTED] certain [REDACTED] contractors had access to raw FISA
information on FBI storage systems [REDACTED] Id. The apparent purpose for the
FBI’s granting such access was to receive analytical assistance from [REDACTED] [REDACTED]
[REDACTED]

[REDACTED] Nonetheless, the [REDACTED] contractors had access to raw
FISA information that went well beyond what was necessary to respond to the FBI’s requests;
[REDACTED]

[REDACTED] The FBI discontinued the above-described access to raw FISA information as of April 18,
2016. [REDACTED]

The contractors in question received training on the FBI minimization procedures, stored
the raw information only on FBI systems, and did not disseminate it further. Id. at 93.
Nonetheless, the above-described practices violated the governing minimization procedures.
Section III.A of the FBI’s minimization procedures (as then in effect and as now proposed)
provides: “The FBI must retain all FISA-acquired information under appropriately secure
conditions that limit access to such information only to authorized users in accordance with these
and other applicable FBI procedures. These retention procedures apply to FISA-acquired
information retained in any form.” The FBI may disseminate Section 702-acquired information
only in accordance with Section V of those procedures. FBI Minimization Procedures § III.C.1.

Under Section V.D of those procedures, personnel working for another federal agency
such as [REDACTED] may receive raw information acquired under Section 702 in order to

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 84

~~TOP SECRET//SI//ORCON/NOFORN~~

provide technical or linguistic assistance to the FBI, but only if certain restrictions are followed.

See id. § V.D. Those restrictions were not in place with regard to the [REDACTED] contractors: their

access was not limited to raw information for which the FBI sought assistance and access

continued even after they had completed work in response to an FBI request. See [REDACTED]

Compliance Report at 93. At the October 4, 2016 Hearing, the government represented that it

was investigating whether there have been similar cases in which the FBI improperly afforded

non-FBI personnel access to raw FISA-acquired information on FBI systems. October 4, 2016

Transcript at 64.

In a separate violation of its minimization procedures, the FBI delivered raw Section 702-acquired information to a [REDACTED] contractor called [REDACTED]

[REDACTED] Compliance Report at 131. The information in question pertains to [REDACTED]

[REDACTED] accounts tasked under Section 702. Id. [REDACTED]

[REDACTED] as a federal agency, could receive raw Section 702-acquired information in order to provide technical assistance to the FBI, subject to the requirements of Section V.D of the FBI Minimization Procedures. See FBI Minimization Procedures § V.D (“FBI is authorized to

~~TOP SECRET//SI//ORCON/NOFORN~~

Page 85

~~TOP SECRET//SI//ORCON//NOFORN~~

disclose FISA-acquired information to assisting federal agencies for further processing and analysis,” subject to specified restrictions) (emphasis added). [REDACTED] however, is not a federal agency and the [REDACTED] personnel who worked with the information were “not directly supervised by or otherwise under the direction and control of [REDACTED] Compliance Report at 132. For these reasons, the government concluded that the FBI had given the information to the private entity [REDACTED], not to an assisting federal agency. See id.⁶⁸

[REDACTED]

The government has not explained why giving [REDACTED] personnel access to the raw information during installation of the tool would not involve a separate violation of the FBI Minimization Procedures. Accordingly, the Court is ordering the government to provide additional information regarding this second grant of access to raw Section 702 information.

These violations, when placed in the context of Section 702 acquisitions in their entirety, do not preclude a finding that the FBI Minimization Procedures meet the statutory definition of “minimization procedures” and are consistent with the requirements of the Fourth Amendment.

⁶⁸ In contrast, the above-described [REDACTED] contractors worked in a federal facility under the supervision of [REDACTED] Compliance Report at 93. It appears that the government views the above-described disclosures of information to the [REDACTED] contractors as disclosures to a federal agency, rather than to a private entity or private individuals. In any event, the government acknowledges that those disclosures were improper for other reasons, so the Court need not reach this question.

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 86

~~TOP SECRET//SI//ORCON//NOFORN~~

The improper access previously afforded the [REDACTED] contractors has been discontinued, while the information disclosed to [REDACTED] pertains to just [REDACTED] tasked selectors.

The Court is nonetheless concerned about the FBI's apparent disregard of minimization rules and whether the FBI may be engaging in similar disclosures of raw Section 702 information that have not been reported.⁶⁹ Accordingly, the Court is directing the government to provide additional as described below.

2. Potential Over-Retention of Section 702 Information

Last year, in the context of approving the standard minimization procedures employed by the FBI for electronic surveillance and physical search conducted under Titles I and III of FISA, a judge of the FISC observed:

FBI personnel who develop storage systems for FISA-acquired information and decide under what circumstances FISA-acquired information is placed on those systems are bound by applicable minimization procedures and FISC orders, no less so than an agent conducting a FISC-authorized physical search or an analyst preparing a report for dissemination.

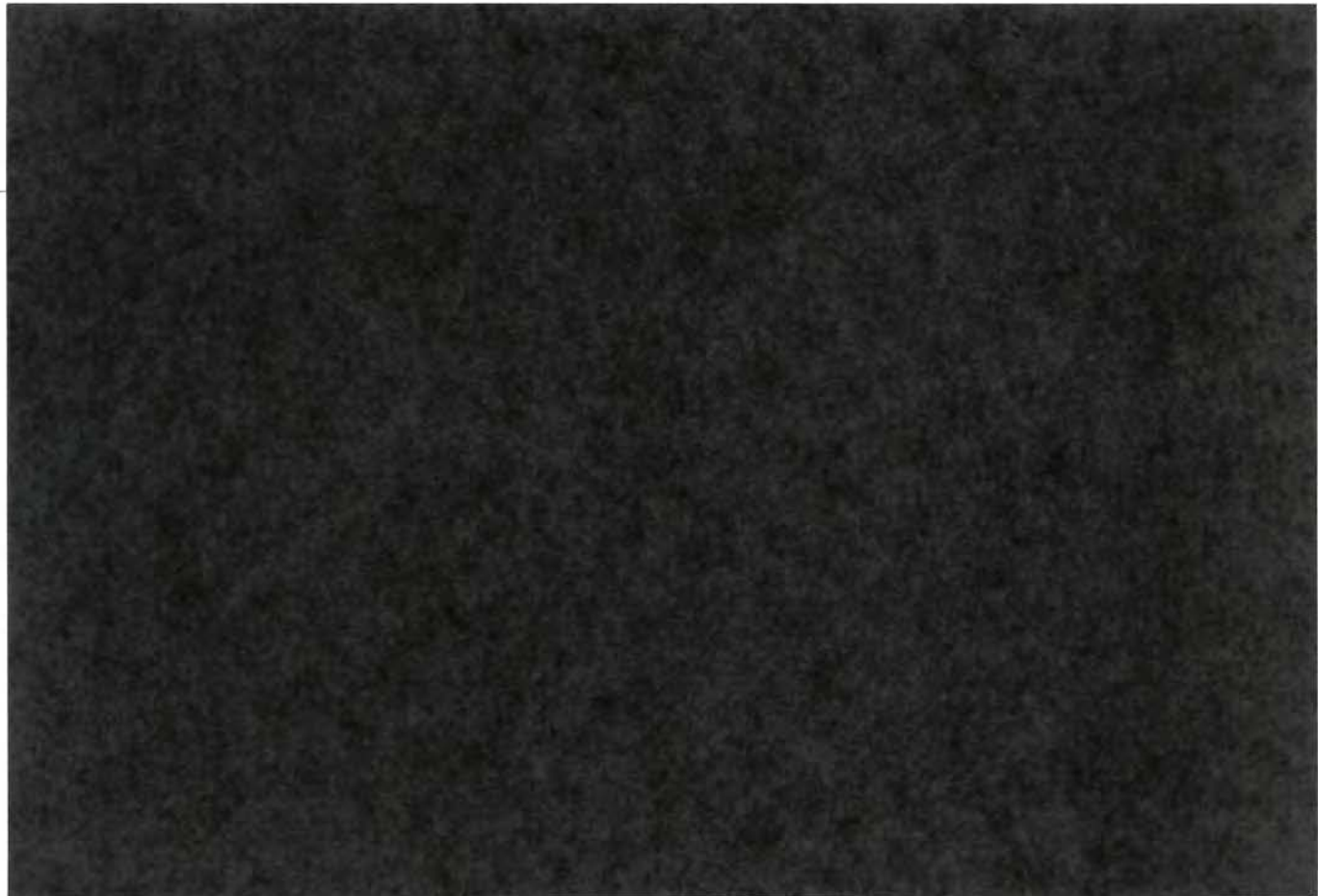
Docket No. [REDACTED], Opinion and Order at 45 (FISA Ct. May 17, 2016). Recent disclosures regarding [REDACTED] systems maintained by the FBI suggest that raw FISA

⁶⁹ The improper access granted to the [REDACTED] contractors was apparently in place [REDACTED] and seems to have been the result of deliberate decisionmaking. [REDACTED] Compliance Report at 92-93 ([REDACTED] access to FBI systems was the subject of an interagency memorandum of understanding entered into [REDACTED]). Despite the existence of an interagency memorandum of understanding (presumably prepared or reviewed by FBI lawyers), no notice of this practice was given to the FISC until 2016. Of course, such a memorandum of understanding could not override the restrictions of Section 702 minimization procedures.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

information, including Section 702 information, may be retained on those systems in violation of applicable minimization requirements. [REDACTED]⁷⁰



The government has not identified the provisions of the FBI Minimization Procedures it believes are implicated by the above-described retention practices. Based on the information

70



~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

provided, however, those practices appear inconsistent with the provisions governing retention on electronic and data storage systems, see FBI Minimization Procedures § III.G.1, on ad hoc systems, id. § IV.A-B, and in connection with litigation, id. § III.G.4. Nearly four months ago, the government undertook to address this indefinite retention of information on the above-described systems in a subsequent filing, see December 29, 2016 Report at 10-11, but has not done so. Accordingly, the Court is directing the government to provide pertinent information, as described below.

3. Review Teams for Attorney-Client Communications

The Section 702 minimization procedures

have specific rules for handling attorney-client communications. Because the FBI has law enforcement responsibilities and often works closely with prosecutors in criminal cases, its procedures have detailed requirements for cases in which a target is known to be charged with a federal crime. Unless otherwise authorized by the [National Security Division of DOJ], the FBI must establish a separate review team whose members have no role in the prosecution of the charged criminal matter to conduct the initial review of such a target's communications. When that review team identifies a privileged communication concerning the charged criminal matter, the original record or portion thereof containing that privileged communication is sequestered with the FISC and other copies are destroyed (save only any electronic version retained as an archival backup, access to which is restricted).

November 6, 2015 Opinion at 47-48 (citations and internal quotation marks omitted).

Failures of the FBI to comply with this "review team" requirement for particular targets have been a focus of the FISC's concern since 2014. See id. at 48-52; August 26, 2014 Opinion at 35-36. The government generally ascribed those failures to misunderstanding or confusion on the part of individuals – for example, when an agent is generally aware of the review team requirement but mistakenly believes that it does not apply when the charging instrument is under

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 89

~~TOP SECRET//SI//ORCON/NOFORN~~

seal. November 6, 2015 Opinion at 50. The government advised that it was emphasizing the review team requirement in ongoing training and oversight efforts, and that such emphasis had resulted in the identification and correction of additional cases in which review teams had not been properly established. Id. at 51.

[REDACTED]

[REDACTED] targets who have been subject to criminal charges [REDACTED] there was a delay of over two years in establishing review teams. See [REDACTED] Preliminary Notice of Compliance Incident Regarding [REDACTED] Section 702-Tasked Facilities (“ [REDACTED] Preliminary Notice”) at 2-3. The primary cause of this delay was that the responsible case agent was unaware of the review team requirement. That agent took the appropriate steps after reviewing an advisory that reminded FBI personnel about the requirement in [REDACTED] Id. at 3.⁷¹ The government also reported a delay of approximately one month during [REDACTED] before establishing a review team after a target was charged in a sealed complaint. The delay appears to have been the result of lack of coordination among FBI field offices. According to the government, the review teams have completed examination of communications acquired prior to

~~TOP SECRET//SI//ORCON/NOFORN~~

Page 90

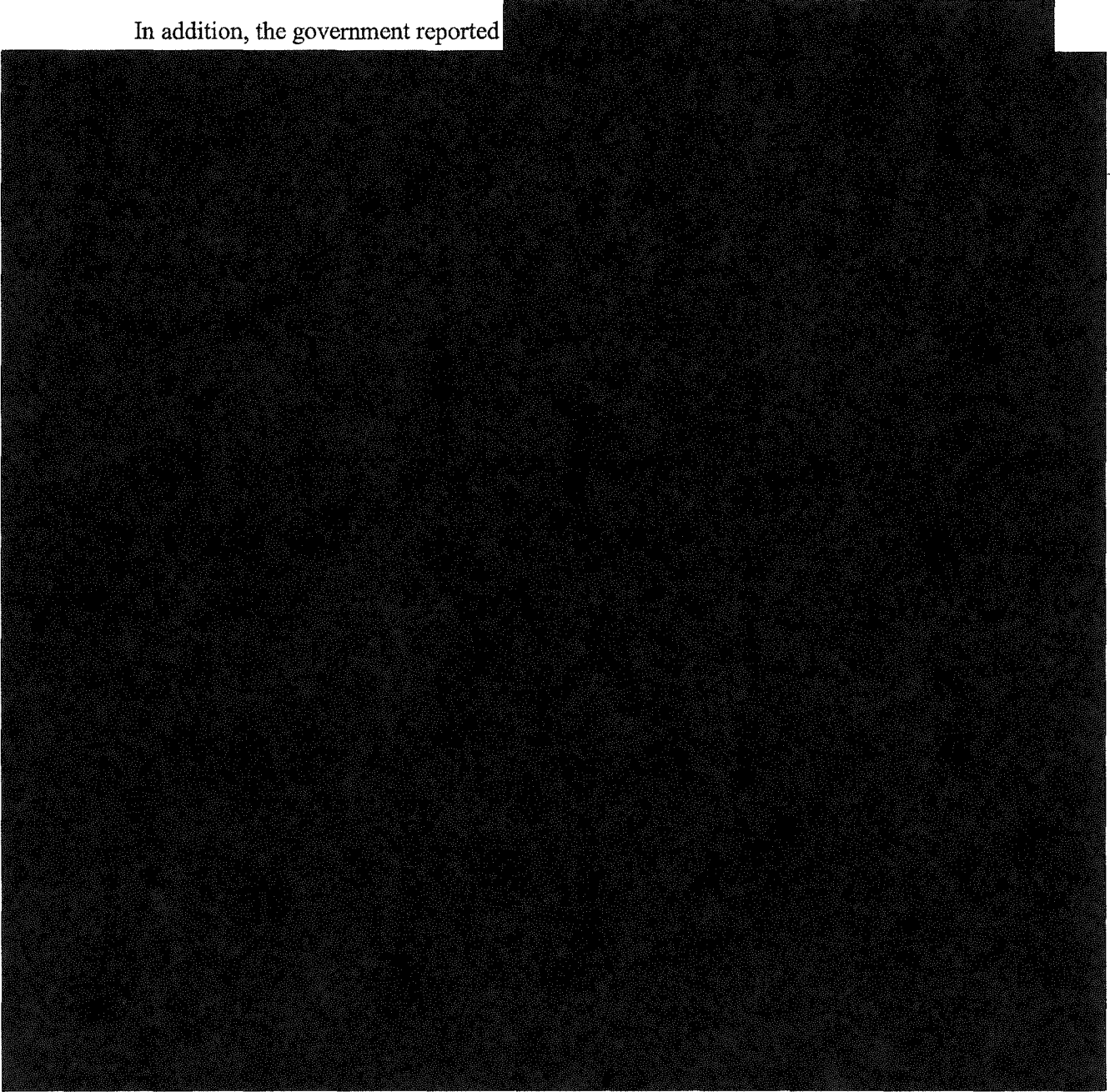
JA2880

~~TOP SECRET//SI//ORCON//NOFORN~~

their creation for both incidents and did not discover any privileged communications. [REDACTED]

[REDACTED] Compliance Report at 77, 105.

In addition, the government reported [REDACTED]



~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~



A separate source of under-inclusiveness is when personnel do not identify and segregate communications for [REDACTED]



[REDACTED] FBI examination of the erroneously-excluded communications is ongoing and, so far, has not identified any attorney-client privileged communications concerning a charged matter. [REDACTED] Compliance Report at 119.

A different [REDACTED] problem affected [REDACTED] [REDACTED] accounts during November 28-30, 2016. That problem has been solved prospectively. Although some communications for

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

those tasked accounts were accessed before being segregated for the review team, none of them contained privileged information. Id. at 83 n.58.

In order to address some of the sources of such under-inclusiveness, the FBI has implemented a new [REDACTED] process for [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] In addition, the FBI and NSA have taken steps to address the difficulties encountered with regard to [REDACTED] Id. at 4.

It seems clear that the review team requirement should continue to be a point of emphasis in the government's training and oversight efforts. The measures taken to improve processes for identifying and routing information subject to the review team requirement appear well-suited to address the described under-inclusiveness problems. In view of those efforts, and the fact that lapses to date appear to have resulted in few, if any, privileged communications concerning charged matters being reviewed by investigators other than review team members, errors in implementing the review team requirements do not preclude a finding that the FBI Minimization Procedures meet the statutory definition of "minimization procedures" and are consistent with the requirements of the Fourth Amendment.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

E. Issues Arising Under the CIA Minimization Procedures

In the course of investigating a separate compliance incident that occurred in December 2016,⁷² the CIA discovered several problems with its purge practices. First, the software script used to identify communications subject to purge requirements within a storage system [REDACTED]

[REDACTED] had not been identifying all communications subject to purge that had been acquired by

[REDACTED] December 28, 2016, Preliminary Notice of Compliance Incidents and Material Misstatements Regarding Collection Pursuant to Title I and Title III and Section 702 of FISA, at 4. As of March 29, 2017, CIA was in the process of remedying the incomplete purges. Supplemental Notice Regarding Incomplete Purges of Collection Acquired Pursuant to Section 702 of FISA, filed on March 29, 2017 (“March 29, 2017 Supp. Notice”) at 2.

Further investigation of the December 2016 incident revealed similar problems with scripts used to purge metadata from [REDACTED] CIA repositories [REDACTED]. March 29, 2017 Supp. Notice at 2-3. The government reports CIA has corrected those script problems and completed the required purges, except for certain information relating [REDACTED] facilities, for which remedial efforts are ongoing. *Id.* at 3 & n.4.

⁷² That incident appears to have been remedied, *see id.* at 3, and in and of itself does not merit discussion in this Opinion.

⁷³ [REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

In late March 2017, also in the course of investigating the December 2016 incident, CIA discovered another form of purging error affecting [REDACTED] March 24, 2017, Notice of Compliance Incident Regarding Incomplete Age Off of Data Acquired Pursuant to Section 702 of FISA at 2. The government is examining the scope of that error. Id.

The government has not advised the Court for how long these various purge-related problems persisted before CIA discovered them in the course of investigating the separate incident. It appears that, having recognized the problems, CIA is taking reasonable steps to address them. Nonetheless, the Court encourages the government to take proactive measures to verify that the automated processes upon which it relies to implement minimization requirements are functioning as intended.

V. CONCLUSION

For the foregoing reasons, the Court finds that: (1) the 2016 Certifications, as amended by the 2017 Amendments, as well as the certifications in the Prior 702 Dockets as amended by those documents, contain all the required statutory elements; (2) the targeting and minimization procedures to be implemented regarding acquisitions conducted pursuant to the 2016 Certifications, as amended by the 2017 Amendments, comply with 50 U.S.C. §1881a(d)-(e) and are consistent with the requirements of the Fourth Amendment; and (3) the minimization procedures to be implemented regarding information acquired under prior Section 702 certifications comply with 50 U.S.C. §1881a(d)-(e) and are consistent with the requirements of the Fourth Amendment. Orders approving the amended certifications and use of the accompanying procedures are being entered contemporaneously herewith.

~~TOP SECRET//SI//ORCON/NOFORN~~

Page 95

~~TOP SECRET//SI//ORCON//NOFORN~~

For the reasons discussed above, it is HEREBY ORDERED as follows:

1. Raw information obtained by NSA's upstream Internet collection under Section 702 shall not be provided to FBI, CIA or NCTC unless it is done pursuant to revised minimization procedures that are adopted by the AG and DNI and submitted to the FISC for review in conformance with Section 702.

2. The government shall take steps to ensure that NCTC retains raw Section 702-acquired information that is determined to be evidence of a crime but not foreign intelligence information beyond the generally applicable age-off period specified in Section B.2 of the NCTC Minimization Procedures only as long as reasonably necessary to serve a law enforcement purpose and that NCTC does not use or disclose such information other than for a law enforcement purpose. The government shall report in writing on such steps when it seeks to renew or amend [REDACTED].

3. On or before December 31 of each calendar year, the government shall submit a written report to the FISC: (a) describing all administrative, civil or criminal litigation matters necessitating preservation by FBI, NSA, CIA or NCTC of Section 702-acquired information that would otherwise be subject to destruction, including the docket number and court or agency in which such litigation matter is pending; (b) describing the Section 702-acquired information preserved for each such litigation matter; and (c) describing the status of each such litigation matter.

4. The government shall promptly submit a written report describing each instance in which FBI, NSA, CIA or NCTC invokes the provision of its minimization procedures stating that

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 96

~~TOP SECRET//SI//ORCON//NOFORN~~

nothing in those procedures shall prohibit the “retention, processing, analysis or dissemination of information necessary to comply with a specific congressional mandate or order of a court within the United States[.]” See NSA Minimization Procedures § 1; CIA Minimization Procedures § 6.g; FBI Minimization Procedures § I.G; NCTC Minimization Procedures § A.6.d. Each such report shall describe the circumstances of the deviation from the procedures and identify the specific mandate on which the deviation was based.

5. The government shall promptly submit a written report describing any instance in which an agency departs from any provision in its minimization procedures in reliance in whole or in part on the provision therein for lawful oversight when responding to an oversight request by an entity other than the oversight entities expressly referenced in the agency’s procedures. See NSA Minimization Procedures § 1; CIA Minimization Procedures § 6.f; FBI Minimization Procedures § I.G; NCTC Minimization Procedures § A.6.e. Each such report shall describe the circumstances of the deviation from the procedures and identify the specific oversight activity on which the deviation was based.

6. No later than June 16, 2017, the government shall submit a written report:
- (a) describing the extent to which raw FISA information, including Section 702 information, is retained:



~~TOP SECRET//SI//ORCON//NOFORN~~

Page 97

JA2887

~~TOP SECRET//SI//ORCON/NOFORN~~

- (b) assessing whether such retention complies with applicable minimization requirements; and
 - (c) to the extent that noncompliance is found, describing the steps the government is taking or plans to take to discontinue the above-described forms of retention or bring them into compliance with applicable minimization requirements.
-

7. No later than June 16, 2017, the government shall submit one or more written reports that provide the following:

- (a) the results of the government's investigation of whether there have been additional cases in which the FBI improperly afforded non-FBI personnel access to raw FISA-acquired information on FBI systems; and
- (b) a description of the installation of the [REDACTED] by [REDACTED] personnel on an FBI system, including:



8. At 90-day intervals, the government shall submit written updates on NSA's implementation of the above-described sequester-and-destroy process to information acquired on or before March 17, 2017, by upstream Internet collection under Section 702.

9. If the government intends not to apply the above-described sequester-and-destroy process to information acquired on or before March 17, 2017, by upstream Internet collection

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

under Section 702 because the information is not contained in an “institutionally managed repository,” it shall describe the relevant circumstances in a written submission to be made no later than June 2, 2017; however, the government need not submit such a description for circumstances referenced in this Opinion and Order as ones in which NSA could retain such information.

10. The government shall promptly submit in writing a report concerning each instance in which FBI personnel receive and review Section 702-acquired information that the FBI identifies as concerning a United States person in response to a query that is not designed to find and extract foreign intelligence information. The report should include a detailed description of the information at issue and the manner in which it has been or will be used for analytical, investigative or evidentiary purposes. It shall also identify the query terms used to elicit the information and provide the FBI’s basis for concluding that the query was consistent with applicable minimization procedures.

ENTERED this 26 day of April, 2017, in Docket Nos. [REDACTED]

[REDACTED]

Rosemary M. Collyer
ROSEMARY M. COLLYER
Judge, United States Foreign
Intelligence Surveillance Court

I, [REDACTED], Chief Deputy Clerk,
FISC, certify that this document is a
true and correct copy of the original.

[REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~

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 5 OF 7 (JA2890–JA3406)

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

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 Defendants–Appellees

*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

U.S. District Court for the District of Maryland, Docket Sheet,
Case No. 1:15-cv-00662JA0001

Plaintiff Wikimedia Foundation’s Amended Complaint
(June 22, 2015), ECF No. 72JA0036

Exhibits to Wikimedia Foundation’s Motion to Compel

Declaration of Patrick Toomey, Counsel for Wikimedia Foundation
(Mar. 26, 2018), ECF No. 125-3JA0096

Exhibit 1: Chart Identifying Discovery Requests at Issue on
Wikimedia Foundation’s Motion to Compel,
ECF No. 125-4.....JA0101

Exhibit 2: Wikimedia Foundation’s Requests for Admission
and attachments (Nov. 7, 2017), ECF No. 125-5.....JA0118

**Exhibits to Defendants’ Opposition
to Wikimedia Foundation’s Motion to Compel**

Declaration of Daniel R. Coats, Director of National Intelligence
(Apr. 28, 2018), ECF No. 138-2.....JA0170

Declaration of Lauren L. Bernick, Senior Associate Civil Liberties
Protection Officer in the Office of Civil Liberties, Privacy, and
Transparency at the Office of the Director of National Intelligence
(Apr. 28, 2018), ECF No. 138-3.....JA0190

Notice of Filing Unclassified & Redacted Version of the Declaration of George C. Barnes, Deputy Director of the NSA (May 11, 2018), ECF No. 141JA0199

Unclassified & Redacted Version of the Declaration of George C. Barnes, Deputy Director of the NSA (May 11, 2018), ECF No. 141-1JA0201

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

Declaration of Ashley Gorski, Counsel for Wikimedia Foundation (May 18, 2018), ECF No. 143-1JA0270

Exhibit 1: Chart Identifying Deposition Questions at Issue on Wikimedia Foundation’s Motion to Compel, ECF No. 143-2.....JA0272

Exhibit 2: Transcript of Deposition of NSA’s Designated Witness, Rebecca J. Richards, Pursuant to Fed. R. Civ. P. 30(b)(6) (Apr. 16, 2018), ECF No. 143-3JA0286

**Opinion & Order
Denying Wikimedia Foundation’s Motion to Compel**

Memorandum Opinion (Aug. 20, 2018), ECF No. 150.....JA0689

Order Denying Plaintiff’s Motion to Compel Discovery Responses & Deposition Testimony (Aug. 20, 2018), ECF No. 151.....JA0716

Exhibits to Defendants’ Motion for Summary Judgment

Declaration of Henning Schulzrinne, Julian Clarence Levi Professor of Computer Science at Columbia University (Nov. 13, 2018), ECF No. 164-4.....JA0719

Declaration of James Gilligan, Counsel for Defendants (Nov. 13, 2018), ECF No. 164-5JA0818

Exhibit 3: Wikimedia Foundation’s Amended and Supplemental Responses and Objections to NSA’s First Set of Interrogatories (Mar. 23, 2018), ECF No. 164-6JA0821

Exhibit 4: Wikimedia Foundation’s Amended Responses and Objections to ODNI’s Interrogatory No. 19 (Apr. 6, 2018), including Technical Statistics Chart, ECF No. 164-7JA0861

Exhibit 5: Wikimedia Foundation’s Responses and Objections to NSA’s First Set of Interrogatories (Jan. 11, 2018), ECF No. 164-8.....JA0876

VOLUME 2

**Exhibits to Wikimedia Foundation’s
Opposition to Defendants’ Motion for Summary Judgment**

Declaration of Scott Bradner, Former Senior Technology Consultant for the Harvard University Chief Technology Officer (Dec. 18, 2018), ECF No. 168-2JA0920

Appendices A through Z to Declaration of Scott Bradner (Dec. 18, 2018), ECF Nos. 168-3 to 168-4JA1067

VOLUME 3

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

Appendices AA through FF to Declaration of Scott Bradner (Dec. 18, 2020), ECF No. 168-5JA1791

Declaration of Jonathon Penney, Associate Professor at the Schulich School of Law and Director of the Law & Technology Institute at Dalhousie University (Dec. 18, 2018), ECF No. 168-6JA2151

Declaration of Michelle Paulson, Former Legal Director and Interim General Counsel for Wikimedia Foundation (Dec. 18, 2018), ECF No. 168-7.....JA2218

Declaration of James Alexander, Former Manager for Trust and Safety and Former Legal and Community Advocacy Manager at Wikimedia Foundation (Dec. 18, 2018), ECF No. 168-8JA2244

Declaration of Tilman Bayer, Senior Analyst for Wikimedia Foundation Product Analytics Team (Dec. 18, 2018), ECF No. 168-9.....JA2253

Declaration of Emily Temple-Wood (Dec. 18, 2018), ECF No. 168-10.....JA2268

Declaration of Patrick Toomey, Counsel for Wikimedia Foundation (Dec. 18, 2018), ECF No. 168-11.....JA2278

Exhibit 8: Wikimedia-hosted email list discussing NSA slide with Wikimedia logo, from July to August 2013, ECF No. 168-12.....JA2283

Exhibit 9: Wikimedia “Talk page” discussing its non-public information policy, from September to December 2013, ECF No. 168-13.....JA2305

Exhibit 10: “OTRS” ticket showing Wikimedia user requesting Tor permissions in September 2013, ECF No. 168-14JA2349

VOLUME 4

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

Exhibit 11: Wikimedia webpage showing Wikimedia user requesting Tor permissions in September 2017, ECF No. 168-15.....JA2353

Exhibit 12: Wikimedia document compiling German-user-

community appeal concerning privacy in 2013,
ECF No. 168-16.....JA2357

Exhibit 13: Wikimedia “Talk page” discussing NSA
surveillance from June to December 2013,
ECF No. 168-17.....JA2363

Exhibit 14: Wikimedia Technical Statistics Chart & Supporting
Exhibits A-G, ECF No. 168-18JA2396

Exhibit 15: Privacy & Civil Liberties Oversight Board, *Report
on the Surveillance Program Operated Pursuant to Section 702
of FISA* (July 2014), ECF No. 168-19.....JA2434

Exhibit 16: FISC Memorandum Opinion, [*Redacted*], 2011 WL
10945618 (Oct. 3, 2011), ECF No. 168-20JA2631

Exhibit 17: Office of the Director of National Intelligence, *DNI
Declassifies Intelligence Community Documents Regarding
Collection Under Section 702 of FISA* (Aug. 21, 2013),
ECF No. 168-21.....JA2717

Exhibit 18: Defendant NSA’s Objections and Responses to
Plaintiff’s First Set of Interrogatories (Dec. 22, 2017),
ECF No. 168-22.....JA2721

Exhibit 19: FISC Submission, *Clarification of National Security
Agency’s Upstream Collection Pursuant to Section 702 of FISA*
(May 2, 2011), ECF No. 168-23JA2743

Exhibit 20: Office of the Director of National Intelligence,
*Statistical Transparency Report Regarding Use of National
Security Authorities, Calendar Year 2017* (Apr. 2018),
ECF No. 168-24.....JA2748

Exhibit 21: FISC Memorandum Opinion & Order
(Apr. 26, 2017), ECF No. 168-25.....JA2790

VOLUME 5

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

Exhibit 22: FISC Submission, *Government’s Response to the Court’s Briefing Order of May 9, 2011* (June 1, 2011), ECF No. 168-26.....JA2890

Exhibit 23: *Big Brother Watch & Others v. United Kingdom*, App. Nos. 58170/13, 62322/14, 24960/15, Eur. Ct. H.R. (2018), ECF No. 168-27.....JA2932

Exhibit 24: NSA Director of Civil Liberties & Privacy Office, *NSA’s Implementation of FISA Section 702* (Apr. 16, 2014), ECF No. 168-28.....JA3145

Exhibit 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), ECF No. 168-29JA3157

Exhibit 26: *Minimization Procedures Used by the NSA in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of FISA* (July 2014), ECF No. 168-30.....JA3193

Exhibit 27: Glenn Greenwald, *XKeyscore: NSA Tool Collects “Nearly Everything a User Does on the Internet,”* Guardian, July 31, 2013, ECF No. 168-31JA3209

Exhibit 28: NSA slide, excerpted from Exhibit 27 (Greenwald, *XKeyscore: NSA Tool Collects “Nearly Everything a User Does on the Internet”*), ECF No. 168-32JA3220

Exhibit 29: Morgan Marquis-Boire, et al., *XKEYSCORE: NSA’s Google for the World’s Private Communications*, Intercept, July 1, 2015, ECF No. 168-33JA3222

Exhibit 30: NSA slide deck, *XKEYSCORE for Counter-CNE*, published in *The Intercept* on July 1, 2015, ECF No. 168-34 ...JA3237

Exhibit 31: Wikimedia, *Founding Principles*
 (accessed Mar. 14, 2018), ECF No. 168-35JA3259

Exhibit 32: Yana Welinder, *Opposing Mass Surveillance on the Internet*, Wikimedia Blog (May 9, 2014), ECF No. 168-36JA3262

Exhibit 33: Wikimedia Public Policy, *Privacy*
 (accessed Mar. 14, 2018), ECF No. 168-37JA3266

Exhibit 34: Wikipedia, *Sock Puppetry*
 (accessed Mar. 14, 2018), ECF No. 168-38JA3273

Exhibit 35: Wikimedia, *Privacy Policy*
 (accessed Feb. 14, 2018), ECF No. 168-39.....JA3286

Exhibit 36: Ryan Lane, *The Future of HTTPS on Wikimedia Projects*, Wikimedia Blog (Aug. 1, 2013),
 ECF No. 168-40.....JA3311

Exhibit 37: Yana Welinder, et al., *Securing Access to Wikimedia Sites with HTTPS*, Wikimedia Blog
 (June 12, 2015), ECF No. 168-41JA3317

Exhibit 38: Wikimedia email describing Tech/Ops goals and
 the importance of HTTPS (May 23, 2014), ECF No. 168-42....JA3325

Exhibit 39: Wikimedia document discussing IPsec
 implementation, including July 8, 2013 statement from a
 Wikimedia engineer, ECF No. 168-43JA3328

Exhibit 40: Wikimedia job posting for Traffic Security
 Engineer (accessed Feb. 8, 2018), ECF No. 168-44JA3364

Exhibit 41: Michelle Paulson, *A Proposal for Wikimedia’s New Privacy Policy and Data Retention Guidelines*, Wikimedia
 Blog (Feb. 14, 2014), ECF No. 168-45JA3367

Exhibit 42: Wikimedia’s Supplemental Exhibit C in response

to NSA Interrogatory No. 8 (volume of HTTP border-crossing communications by country), ECF No. 168-46JA3375

Exhibit 43: Wikimedia’s Supplemental Exhibit D in response to NSA Interrogatory No. 8 (volume of HTTPS border-crossing communications by country), ECF No. 168-47JA3388

Exhibit 44: Wikimedia analytics document showing monthly unique visitors to Wikimedia by region, from December 2007 to May 2015, ECF No. 168-48JA3400

Exhibit 45: Press Release, NSA, *NSA Stops Certain Section 702 “Upstream” Activities*, Apr. 28, 2017, ECF No. 168-49.....JA3404

VOLUME 6

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

Second Declaration of Henning Schulzrinne, Julian Clarence Levi Professor of Computer Science at Columbia University (Feb. 15, 2019), ECF No. 178-2JA3407

Declaration of Alan J. Salzberg, Principal of Salt Hill Statistical Consulting (Feb. 15, 2019), ECF No. 178-3JA3452

Second Declaration of James Gilligan, Counsel for Defendants (Feb. 15, 2019), ECF No. 178-4JA3725

Exhibit 9: Wikimedia Foundation’s Responses and Objections to DOJ’s First Set of Interrogatories (Jan. 11, 2018), ECF No. 178-5.....JA3728

Exhibit 10: Relevant Portions of the Deposition of James Alexander, Wikimedia Foundation witness taken pursuant to Fed. R. Evid. 30(b)(6), ECF No. 178-6JA3761

Exhibit 11: Relevant Portions of the Deposition of Michelle

Paulson, Wikimedia Foundation witness taken pursuant to
 Fed. R. Evid. 30(b)(6), ECF No. 178-7JA3777

Exhibit 12: Wikimedia Foundation, *Securing access to
 Wikimedia sites with HTTPS*, June 12, 2015
 (WIKI0007108-7114), ECF No. 178-8JA3791

Exhibit 13: Wikipedia: Village pump (technical)/Archive 138
 (WIKI0006872-6938), ECF No. 178-9JA3800

Exhibit 14: Jimmy Wales and Lila Tretikov, “Stop Spying on
 Wikimedia Users,” N.Y. Times, Mar. 10, 2015,
 ECF No. 178-10.....JA3869

Exhibit 15: Wikimedia Foundation, *Wikimedia v. NSA:
 Wikimedia Foundation files suit against NSA to challenge
 upstream mass surveillance*, Mar. 10, 2015,
 ECF No. 178-11.....JA3873

VOLUME 7

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

Second Declaration of Scott Bradner, Former Senior Technology
 Consultant for the Harvard University Chief Technology Officer
 (Mar. 8, 2019), ECF No. 181-1JA3879

Second Declaration of Jonathon Penney, Associate Professor at the
 Schulich School of Law and Director of the Law & Technology
 Institute at Dalhousie University (Mar. 8, 2019), ECF No. 181-2JA3940

Second Declaration of Michelle Paulson, Former Legal Director
 and Interim General Counsel for Wikimedia Foundation
 (Mar. 8, 2019), ECF No. 181-3JA4006

Second Declaration of Tilman Bayer, Senior Analyst for Wikimedia
 Foundation Product Analytics Team (Mar. 8, 2019),
 ECF No. 181-4.....JA4012

Second Declaration of Emily Temple-Wood (Mar. 8, 2019),
ECF No. 181-5JA4015

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

Third Declaration of Henning Schulzrinne, Julian Clarence Levi
Professor of Computer Science at Columbia University
(Mar. 22, 2019), ECF No. 182-2JA4019

Second Declaration of Alan J. Salzberg, Principal of Salt Hill
Statistical Consulting (Mar. 22, 2019), ECF No. 182-3JA4048

**Opinion & Order
Granting Defendants’ Motion for Summary Judgment**

Memorandum Opinion (Dec. 16, 2019), ECF No. 188JA4073

Order Granting Defendants’ Motion for Summary Judgment
(Dec. 16, 2019), ECF No. 189JA4123

Wikimedia Foundation’s Notice of Appeal

Notice of Appeal (Feb. 14, 2020), ECF No. 191JA4124

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 22

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

GOVERNMENT'S RESPONSE TO THE COURT'S BRIEFING ORDER OF MAY 9, 2011

1. The government's May 2 Letter can be read to take the position that [REDACTED] are communications authorized for collection under the Section 702 Certifications that have previously been approved by the Court. ~~(TS//SI//NF)~~
 - a. For how long has NSA been acquiring [REDACTED] through its upstream collection? ~~(TS//SI//NF)~~

Under the Section 702 Certifications, NSA acquires, *inter alia*, "Internet communications." *E.g.*, DNI/AG 702(g) Certification [REDACTED] Affidavit of General Keith B. Alexander, Director, National Security Agency (NSA), filed Apr. 20, 2011, at ¶ 4. As described by General Alexander, Internet communications "include, but are not limited to, [REDACTED]"

E.g., id. ~~(TS//SI//NF)~~

In the context of NSA's upstream collection techniques, NSA acquires Internet communications in the form of "transactions," which in this filing refers to 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.¹ A "transaction" might contain information or data representing either a discrete communication (e.g., an e-mail message), or multiple discrete communications [REDACTED]. As further described in the response to question 2 below, whenever a tasked selector is present within a transaction, NSA's "upstream" Internet collection techniques are designed to identify and acquire that transaction. ~~(TS//SI//NF)~~

¹ While the terms "Internet communication" and "transmission" have been used to describe the types of communications NSA acquires, NSA believes that, in the context of upstream collection, "transaction" is the more precise term from a technical perspective, because "transmission" could be understood to mean all data being exchanged on the Internet within a specific time period by a specific device, and an "Internet communication" may actually contain multiple logically separate communications between or among persons. ~~(TS//SI//NF)~~

The transactions discussed herein -- whether they contain single or multiple discrete communications having a commonality of a single user -- should not be confused with the two [REDACTED] compliance incidents initially reported to the Court on April 19, 2011, and further discussed below in the Government's response to question 6, which involved the unrelated communications [REDACTED]. ~~(TS//SI//NF)~~

~~Derived From: NSA/CSSM 1-52~~

~~Dated: 20070108~~

~~Declassify On: 20360501~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

At the time of acquisition, NSA's upstream Internet collection devices are, with limited exceptions further described below, not presently 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 may be to, from, or about a tasked selector.² Thus, in order to acquire transactions containing one or more communications to, from, or about a tasked selector, it has been necessary for NSA to employ these same upstream Internet collection techniques throughout the entire timeframe of all certifications authorized under Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended (hereinafter "FISA" or "the Act"), and the Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (Aug. 5, 2007) (hereinafter "PAA"). It was also necessary for NSA to employ these upstream collection techniques to implement the electronic surveillance authorized in *In re*

[REDACTED] Docket No. [REDACTED] and *In re* [REDACTED]

Docket No. [REDACTED] (~~TS//SI//NF~~)

- b. According to the May 2 Letter, [REDACTED] may include the full content of email messages that are not to, from or about the user of a targeted selector. They also may include discrete communications as to which all communicants are within the United States. Please explain how the acquisition of such transmissions: (~~TS//SI//NF~~)
- i. comports with the government's representations to the Court regarding the scope of upstream collection under Section 702 and the approvals granted by the Court in reliance upon those representations in Dockets 702(i) 08-01, [REDACTED] (see, e.g., Docket No. 702(i)-08-01, Aug. 27, 2008 Hearing Transcript at 19-26, 40-41 and Sept. 4, 2008 Memorandum Opinion at 15-20, 38); (~~TS//SI//NF~~)

The Government has concluded, after a careful review of the record, that its prior representations to the Court 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 collection techniques. The Government will attempt through this filing to provide the Court with a more thorough explanation of this technically complex collection. This notwithstanding, the Government respectfully submits that for the reasons set forth in its responses to questions 2.ii.,

² Specifically, as is discussed in the Government's response to questions 2(c) and (d) of the Court's briefing order, NSA does have the ability to identify and acquire discrete communications to, from, or about a tasked selector in certain cases [REDACTED]

[REDACTED] (~~TS//SI//NF~~)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

2.iii., and 5 below, NSA's prior and ongoing acquisition of information utilizing its upstream collection techniques is consistent with the Court's prior orders, meets the requirements of Section 702, and is consistent with the Fourth Amendment. ~~(TS//SI//NF)~~

b. According to the May 2 Letter, [REDACTED] may include the full content of email messages that are not to, from or about the user of a targeted selector. They also may include discrete communications as to which all communicants are within the United States. Please explain how the acquisition of such transmissions: ~~(TS//SI//NF)~~

ii. meets the requirements of Section 702, including, but not limited to, the requirement that targeting procedures must be 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 acquisition to be located in the United States"; and, ~~(TS//SI//NF)~~

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 LOCATED IN THE UNITED STATES. (S)

Under Section 702, the Government targets "persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. § 1881a(a). The Government determines whether the targeting of a person is consistent with Section 702 by applying Court-approved targeting procedures. 50 U.S.C. § 1881a(d). These targeting procedures must be "reasonably designed to (A) ensure that any acquisition authorized under subsection [702(a)] is limited to targeting persons reasonably believed to be located outside the United States; and (B) 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." 50 U.S.C. § 1881a(d)(1). (U)

A. The User of a Tasked Selector is the Person Being Targeted by all Acquisitions by NSA's Upstream Collection, Including Transactions That Contain Multiple Discrete Communications—~~(TS//SI//NF)~~

As previously explained to the Court, the Government "targets" a person by tasking for collection a "selector" (e.g., an e-mail account) believed to be used by that person. *See, e.g., In re DNI/AG Certification* [REDACTED] Docket No. 702(i)-08-01, Mem. Op. at 8 (USFISC Sept. 4, 2008) (hereinafter "[REDACTED] Mem. Op."). NSA acquires foreign intelligence information through the tasking of selectors by collecting communications to or from a selector used by a targeted person (hereinafter "to/from communications") and by collecting communications that refer to or are about a selector used by a targeted person (hereinafter "abouts communications"). *Id.*

~~(TS//SI//NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

In both of these types of acquisition, 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. Specifically, "the persons targeted by acquisition of to/from communications are the users of the tasked selectors," because "their communications are intentionally selected for acquisition." ██████████ Mem. Op. at 15. Similarly, the person being targeted by acquisition of abouts communications is also the user of the tasked selector, "because the government's purpose in acquiring abouts communications is to obtain information about that user." *Id.* at 18 (citation omitted). ~~(TS//SI//NF)~~

This remains true for all acquisitions conducted by NSA's upstream collection -- including transactions containing several discrete communications, only one of which may be to, from, or about the user of a tasked selector. As discussed above, the fact that there also may be communications to, from, or about persons other than the target in the transaction does not mean that those persons are also being targeted by the acquisition. 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 subjected to NSA's targeting procedures.³ 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.* ██████████ 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. United States v. Bin Laden*, 126 F. Supp. 2d 264, 281 (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) (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"). ~~(TS//SI//OC,NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

B. 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 (S)

In conducting acquisitions targeting the user of a tasked selector, the Government "may not intentionally acquire 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." 50 U.S.C. § 1881a(b)(4). As noted above, the targeting procedures must be reasonably designed to prevent such intentional acquisitions. With respect to to/from communications, "because a user of a tasked selector is a party to every to/from communication acquired by NSA, a reasonable belief that the users of tasked selectors are outside the United States will ensure that NSA does not intentionally acquire any to/from communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States." [REDACTED] Mem. Op. at 15 (citation omitted). With respect to upstream collection that may contain abouts communications, NSA's targeting procedures provide that:

[REDACTED]

E.g., Amendment 1 to DNI/AG 702(g) Certification [REDACTED] Docket No. 702(i)-[REDACTED] Ex. A, filed Aug. 12, 2010, at 1-2 (hereinafter "NSA Targeting Procedures"). Although these provisions on their face suggest separate technical means might apply only to the "abouts" aspect of NSA's upstream collection, in practice these provisions currently apply to any Internet transaction collected upstream. (TS//SI//OC,NF)

The Government has previously represented that "the operation of the IP address filters or [REDACTED] prevents the intentional acquisition of communications about the target as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States." *In re DNI/AG 702(g) Certification* [REDACTED] Docket No. 702(i)-08-01, Government's Preliminary Response to Questions Posed by the Court, filed Aug. 26, 2008, at 3. The Government also has represented that these IP filters "have been effective in limiting the collection to communications with at least one communicant located outside the United States."

⁴ This provision has remained identical throughout every set of NSA's Section 702 targeting procedures approved for use by the Court, and is also the same in the proposed targeting procedures submitted with DNI/AG 702(g) Certification [REDACTED] (S//OC,NF)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Id. at 4. Except in one circumstance previously reported to the Court,⁵ the Government is not aware of a case where an about collection resulted in the acquisition of a communication where both ends were inside the United States. NSA therefore continues to believe that these prior representations remain accurate. Accordingly, for the reasons described below, the Government respectfully submits that NSA's targeting procedures are reasonably designed to prevent, in the context of NSA's upstream collection, "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," including Internet communications [REDACTED] that have not been previously described to the Court. 50 U.S.C. § 1881a(d)(1)(B). ~~(TS//SI//OC,NF)~~

1. How NSA's IP Filters Work ~~(S)~~

NSA acquires Internet communications by collecting the individual packets of data that make up those communications. [REDACTED]

[REDACTED]

~~(TS//SI//OC,NF)~~

[REDACTED]

⁵ [REDACTED]

~~(TS//SI//NF)~~

⁶ [REDACTED]

~~(TS//SI//NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

[REDACTED]

(TS//SI//OC,NF)

[REDACTED]

Additionally, at the time of acquisition, NSA's upstream Internet collection devices are, with limited exceptions further described below, not presently capable of distinguishing transactions containing only a single discrete communication to, from or about a targeted selector from transactions containing multiple discrete communications.⁷ Accordingly, NSA cannot prevent the acquisition of, or even mark for separate treatment, those types of transactions that may feature multiple discrete communications [REDACTED]. (TS//SI//OC,NF)

[REDACTED]

⁷ See Government's response to questions 2(c) and (d) *infra*. (U)

[REDACTED]

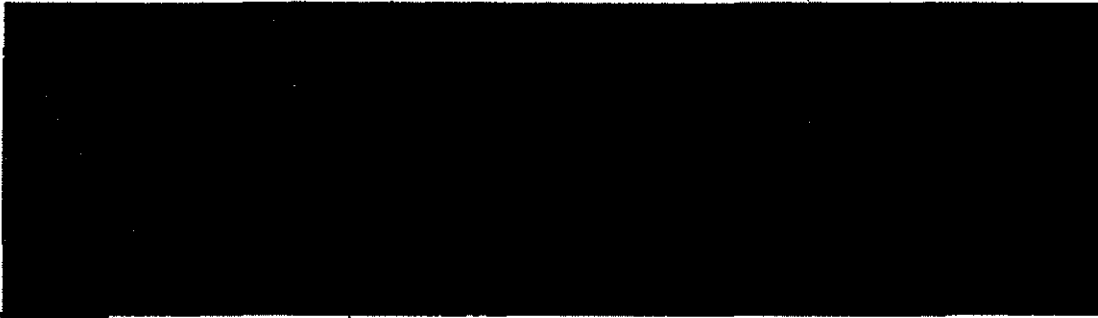
(TS//SI//NF)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~



¹⁰ ~~(TS//SI//OC,NF)~~

Except for the one instance noted above concerning an error by an electronic communication service provider, NSA is not aware of any instance in which its upstream collection on [redacted] or are subject to an IP filter nevertheless resulted in the acquisition of a communication as to which the sender and all intended recipients were known at the time of acquisition to be located in the United States.¹¹ This includes those situations in which NSA might collect unrelated communications when acquiring Internet communications that include multiple, discrete communications. ~~(TS//SI//NF)~~



~~(TS//SI//OC,NF)~~



~~(TS//SI//OC,NF)~~

¹¹ It is noteworthy that the provider error that resulted in the acquisition of domestic communications was first identified not by the provider, but by an NSA analyst who recognized a domestic communication in NSA's repositories, realized that such a domestic communication should not have been acquired, and properly reported the communication through NSA channels. NSA investigated this matter and found that domestic communications had been acquired not due to any theoretical limitations in its IP filter technology, but instead because [redacted]. The domestic overcollection caused by this incident represented a very small portion of NSA's collection during the time period of the overcollection, and an even smaller portion of NSA's collection since the initiation of its Section 702 acquisitions, but the error was still discovered and remedied. It is therefore particularly noteworthy that no NSA analyst has otherwise yet discovered a wholly domestic communication in NSA's repositories collected through NSA's upstream collection systems.

~~(TS//SI//OC,NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

In May 2011, NSA conducted two tests of its Section 702 upstream collection in order to determine the likelihood of collecting an Internet transaction between a user in the United States and [REDACTED]. The first test included [REDACTED]

[REDACTED]
The second test included [REDACTED]
[REDACTED]

~~(TS//SI//NF)~~

The first test sample included no records where both the sender and receiver IP addresses were in the United States [REDACTED]

[REDACTED] NSA analysis further revealed that only [REDACTED] of the more than [REDACTED] (0.028%) had characteristics consistent with a person in the United States accessing a [REDACTED]

[REDACTED]

For the second dataset, NSA analysis discovered that only [REDACTED] out of more than [REDACTED] total records (0.0016%) included a non-targeted user likely accessing the Internet from an IP address in the United States. [REDACTED]

[REDACTED] NSA assesses, based on analysis of the underlying data, that this activity in fact was [REDACTED] copies of the same Internet transaction, [REDACTED]

[REDACTED] There is no indication that NSA collected any wholly domestic communications through its acquisition of this transaction.

~~(TS//SI//NF)~~

In sum, the Government submits that the two test samples discussed above, coupled with the fact that, except as noted above, no NSA analyst has yet discovered in NSA's repositories a wholly domestic communication collected through NSA's upstream collection systems, strongly suggests that NSA's acquisition of transactions or single Internet communications between users in the United States and [REDACTED] currently occurs only in a very small percentage of cases. Even those rare cases, moreover, won't necessarily involve a user in the United States receiving from the [REDACTED] a transaction containing a communication from a person known at the time of acquisition to be located in the United States.¹² ~~(TS//SI//NF)~~

¹² Additionally, as discussed elsewhere herein, even if the sender is located in the United States, the communication likely will not contain any reliable information that would enable NSA to determine at the time of acquisition the sender's location. ~~(TS//SI//OC,NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

2. The [REDACTED] Means by Which NSA Prevents the Intentional Acquisition of Communications as to Which the Sender and All Intended Recipients Are Known to be Located In the United States at the Time of Acquisition Are Reasonable (S)

This Court has found that NSA's targeting procedures are reasonably designed to prevent the intentional acquisition of communications in which the sender and all intended recipients are known at the time of acquisition to be located in the United States. In approving DNI/AG 702(g) Certification [REDACTED], with respect to NSA's upstream collection of "abouts" communications, in particular, the Court noted that NSA "relies on [REDACTED] means of ensuring that at least one party to the communication is located outside the United States." [REDACTED] Mem. Op. at 19. As described above, those [REDACTED] means are NSA's use of "an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas" and NSA's [REDACTED] NSA

Targeting Procedures at 1-2; see also [REDACTED] Mem. Op. at 19. Relying on the Government's representations that these [REDACTED] means had prevented the acquisition of wholly domestic communications under the PAA, and recognizing that it is "theoretically possible that a wholly domestic communication could be acquired as a result of the [REDACTED]" the Court 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." [REDACTED] Mem. Op. at 20 & n.17. The Government respectfully submits that there is no aspect of NSA's upstream collection, as further described herein, that would 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)~~

Two aspects of NSA's upstream collection activity that have not been specifically addressed by the Court are discussed herein: first, the fact that NSA acquires some communications [REDACTED]

and second, the fact that NSA could acquire [REDACTED] -- whether retrieving a single, discrete communication, or a transaction containing several discrete communications -- possibly resulting in the acquisition of wholly domestic communications. ~~(TS//SI//OC,NF)~~

a. Acquisition of Communications that [REDACTED]

(S)

First, [REDACTED]

-- 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 located in the United

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

States.

[REDACTED]

(TS//SI//OC,NF)

b. **Theoretical Acquisition of Wholly Domestic Communications Through**

[REDACTED]

(TS//SI//NF)

With respect to the above-discussed theoretical cases in which NSA could acquire a [REDACTED] NSA's targeting procedures also 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 located in the United States. As discussed above, NSA assesses that [REDACTED]

[REDACTED] only in a minute percentage of cases. Yet even in those rare cases, there would be no way for NSA to know at the time of acquisition that the sender and intended recipient are located in the United States. [REDACTED]

[REDACTED] NSA cannot at that point know the location of the intended recipient, who has yet to receive the message. Likewise, [REDACTED]

[REDACTED] it is highly unlikely that the communication would contain information useful in determining the sender's true location.¹³ In any event, it is currently not possible for NSA's IP filters to [REDACTED]

[REDACTED] Because NSA's filters will be looking at the best available information, [REDACTED] it cannot be said that the sender and all intended recipients of those communications are known at the time of acquisition to be located in the United States. Similarly, in the case of NSA's [REDACTED]

13

(TS//SI//OC,NF)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~



(TS//SI//OC,NF)

Accordingly, NSA has designed its systems so that it should never intentionally acquire a communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States. To the extent that NSA does unintentionally acquire such communications, NSA must treat those communications in accordance with its minimization procedures -- just as it must for other types of communications that it is prohibited from intentionally collecting under subsection 702(b), but nevertheless sometimes does unintentionally acquire, such as communications acquired from a target while that target is located inside the United States. (TS//SI//OC,NF)

c. Conclusion (U)

Although for different reasons than those discussed above, the Court has recognized that it is "theoretically possible that a wholly domestic communication could be acquired" through NSA's upstream collection of "abouts" communications. ██████████ Mem. Op. at 20 n.17. For the reasons outlined above, the Government respectfully submits that, despite the theoretical scenarios under which NSA could acquire communications through its upstream collection as to which the sender and all intended recipients are located in the United States, NSA's targeting procedures are reasonably designed to prevent such acquisitions where the location of the sender and all intended recipients is known at the time of acquisition. (TS//SI//OC,NF)

The remainder of this page intentionally left blank.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release,

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

b. According to the May 2 Letter, [REDACTED] may include the full content of email messages that are not to, from or about the user of a targeted selector. They also may include discrete communications as to which all communicants are within the United States. Please explain how the acquisition of such transmissions: ~~(TS//SI//NF)~~

iii. is consistent with the Fourth Amendment. ~~(TS//SI//NF)~~

NSA's ACQUISITION OF TRANSACTIONS CONTAINING MULTIPLE DISCRETE COMMUNICATIONS IS CONSISTENT WITH THE FOURTH AMENDMENT.
~~(TS//SI//NF)~~

Section 702 requires the Attorney General (AG) and the Director of National Intelligence (DNI) to execute a certification attesting, among other things, that the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment. 50 U.S.C. § 1881a(g)(2)(A)(iv). In reviewing a certification, Section 702 in turn requires the Court to enter an order approving the certification and the use of the targeting and minimization procedures if the Court finds, among other things, that those procedures are consistent with the requirements of the Fourth Amendment. *Id.* § 1881a(i)(3)(A). 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. *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1012 (Foreign Int. Surv. Ct. Rev. 2008) (hereinafter "*In re Directives*"). ~~(TS//SI//NF)~~

The Fourth Amendment protects the right "to be secure . . . against unreasonable searches and seizures" and directs that "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." U.S. Const. amend. IV. As demonstrated below, the Fourth Amendment requires no warrant here, and the upstream collection conducted by NSA is a reasonable exercise of governmental power that satisfies the Fourth Amendment. ~~(TS//SI//NF)~~

A. The Warrant Requirement Does Not Apply to NSA's Acquisition of Transactions Containing Multiple Discrete Communications. ~~(TS//SI//NF)~~

The Supreme Court has recognized exceptions to the Fourth Amendment's warrant requirement "when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable." *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987) (internal quotations omitted); see also *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995) (quoting *Griffin*). The Foreign Intelligence Surveillance Court of Review, in upholding the Government's implementation of the PAA, held that a foreign intelligence exception exists "when surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

believed to be located outside the United States." *In re Directives*, 551 F.3d at 1012. See also *In re Sealed Case*, 310 F.3d 717, 742 (Foreign Int. Surv. Ct. Rev. 2002) ("[A]ll the . . . courts to have decided the issue [have] held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information."). ~~(TS//SI//NF)~~

In approving a previous Section 702 certification, this Court has found that Section 702 acquisitions "fall within the exception recognized by the Court of Review" in that they "target persons reasonably believed to be located outside the United States who will have been assessed by NSA to possess and/or to be likely to communicate foreign intelligence information concerning a foreign power authorized for acquisition under the Certification" and are "conducted for national security purposes." ~~██████████~~ Mem. Op. at 35 (citations omitted). Specifically, this Court recognized that the Court of Review's rationale for applying a foreign intelligence exception "appl[ies] with equal force" to Section 702 acquisitions, in that the Government's purpose in conducting Section 702 acquisitions goes well beyond a normal law enforcement objective and involves "the acquisition from overseas foreign agents of foreign intelligence to help protect national security," a circumstance ~~in which the government's interest is particularly intense.~~ *Id.* at 35-36 (quoting *In re Directives*, 551 F.3d at 1011). In addition, this Court, noting the likely volume of Section 702 acquisitions and the fact that those acquisitions involve targets who are attempting to conceal their communications, found that "[s]ubjecting ~~██████████~~ number of targets to a warrant process inevitably would result in delays and, at least occasionally, in failures to obtain perishable foreign intelligence information, to the detriment of national security." ~~██████████~~ Mem. Op. at 36; see also *United States v. Truong Dinh Hung*, 629 F.2d 908, 913 (4th Cir. 1980) ("attempts to counter foreign threats to the national security require the utmost stealth, speed, and secrecy" such that "[a] warrant requirement would add a procedural hurdle that would reduce the flexibility of executive foreign intelligence initiatives, [and] in some cases delay executive response to foreign intelligence threats..."). The Court's previous finding that the foreign intelligence exception applies to Section 702 acquisitions remains equally applicable here. ~~(TS//SI//NF)~~

B. NSA's Acquisition of Transactions Containing Multiple Discrete Communications is Reasonable Under the Fourth Amendment. ~~(TS//SI//NF)~~

Where, as here, the foreign intelligence exception applies, "governmental action intruding on individual privacy interests must comport with the Fourth Amendment's reasonableness requirement." *In re Directives*, 551 F.3d at 1012. In evaluating the reasonableness of the Government's action, a court must consider the totality of the circumstances, see *United States v. Knights*, 534 U.S. 112, 118 (2001), taking into account "the nature of the government intrusion and how the intrusion is implemented." *In re Directives*, 551 F.3d at 1012 (citing *Tennessee v. Garner*, 471 U.S. 1, 8 (1985) and *United States v. Place*, 462 U.S. 696, 703 (1983)). In balancing these interests, the Court of Review has observed that "[t]he more important the government's interest, the greater the intrusion that may be constitutionally tolerated." *In re Directives*, 551 F.3d at 1012 (citing *Michigan v. Summers*, 452 U.S. 692, 701-05 (1981)). "If the protections that are in place for individual privacy interests are sufficient in light of the governmental interests at stake, the constitutional scales will tilt in favor of upholding the government's actions." *Id.* ~~(TS//SI//NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

1. NSA's Acquisition of Transactions Containing Multiple Discrete Communications Implicates Fourth Amendment-Protected Interests.

~~(TS//SI//NF)~~

Although targeting under Section 702 is limited to non-United States persons reasonably believed to be located outside the United States, who are not entitled to protection under the Fourth Amendment, *see, e.g.*, ██████████ Mem. Op. at 37, this Court has recognized that conducting acquisitions under Section 702 creates a "real and non-trivial likelihood of intrusion on Fourth Amendment-protected interests" of United States persons or persons located in the United States who, for example, communicate directly with a Section 702 target, *id.* at 38.¹⁴ In particular, as described herein, 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. ~~(TS//SI//NF)~~

2. The Government's Interest in the Foreign Intelligence Information Contained in All Transactions, Including Those Containing Multiple Discrete Communications, is Paramount. ~~(TS//SI//NF)~~

On the other side of the ledger, it is axiomatic that the Government's interest in obtaining foreign intelligence information to protect the Nation's security and conduct its foreign affairs is paramount. *See, e.g., Haig v. Agee*, 453 U.S. 280, 307 (1981) ("[I]t is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation." (citations omitted)). Equally indisputable is the Government's interest in conducting acquisitions of foreign intelligence information¹⁵ under Section 702 of the Act. *See* ██████████ Mem. Op. at 37

¹⁴ Although the scope of Fourth Amendment protection for e-mail is not settled, the Government has argued before this Court that United States persons have a reasonable expectation of privacy in the content of such electronic communications. *See, e.g., United States of America's Supplemental Brief on the Fourth Amendment*, Docket No. 105B(g) 07-01, filed Feb. 15, 2008, at 1. The Government likewise assumes for purposes of this filing that the collection of ██████████ implicates privacy interests protected by the Fourth Amendment. ~~(TS//SI//NF)~~

¹⁵ "Foreign intelligence information" is defined as:

- (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.

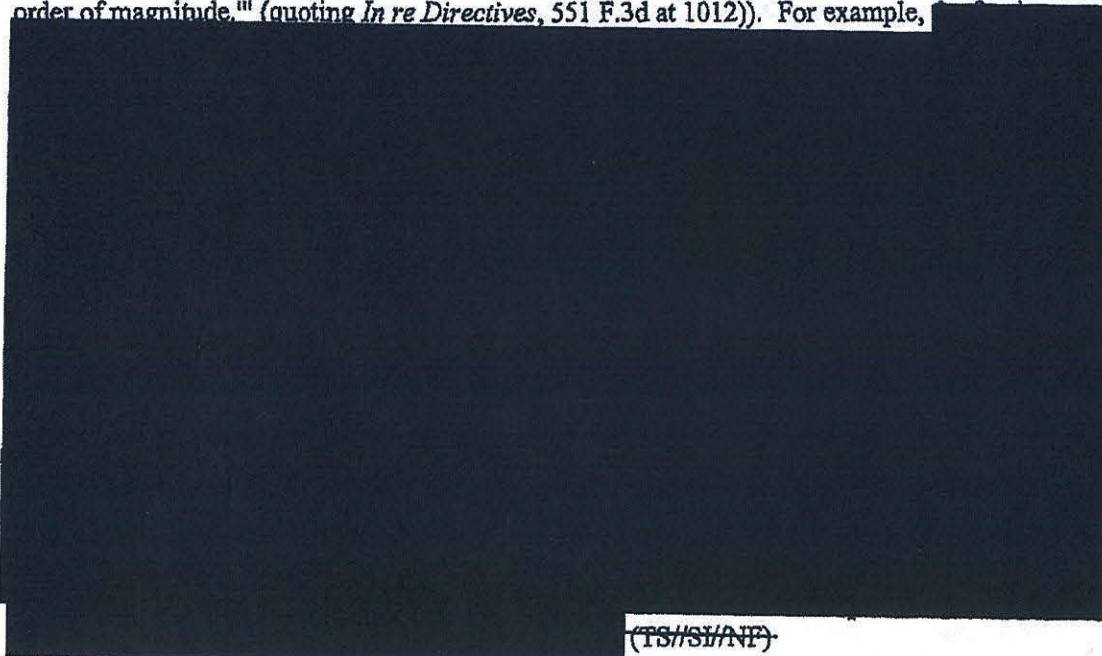
~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

("The government's national security interest in conducting these acquisitions 'is of the highest order of magnitude.'" (quoting *In re Directives*, 551 F.3d at 1012)). For example,



The Supreme Court has indicated that in addition to examining the governmental interest at stake, some consideration of the efficacy of the search being implemented -- that is, some measure of fit between the search and the desired objective -- is also relevant to the reasonableness analysis. See, e.g., *Knights*, 534 U.S. at 119 (noting that the reasonableness of a search "is determined by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which [the search] is needed for the promotion of legitimate governmental interests." (internal quotation marks omitted)); see also *Board of Educ. v. Earls*, 536 U.S. 822, 834 (2002) ("Finally, this Court must consider the nature and immediacy of the government's concerns and the efficacy of the Policy in meeting them.")). Here, NSA's acquisition of transactions through upstream collection is an essential and irreplaceable means of acquiring valuable foreign intelligence information that promotes the paramount governmental interest of protecting the Nation and conducting its foreign affairs.

~~(TS//SI//NF)~~

The AG and DNI have attested that a significant purpose of all acquisitions under Section 702, which includes those conducted by NSA's upstream collection, is to obtain foreign intelligence information. These acquisitions are 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

50 U.S.C. § 1801(e). (U)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

afford a degree of particularity that is reasonable under the Fourth Amendment." [REDACTED] Mem. Op. at 39-40 (footnote omitted). Indeed, certain of the valuable foreign intelligence information NSA seeks to acquire through upstream collection of transactions simply cannot be acquired by any other means. (TS//SI//NF)

Specifically, as this Court has recognized, NSA's upstream collection "is particularly important because it is *uniquely capable* of acquiring certain types of targeted communications containing valuable foreign intelligence information," such as [REDACTED]

[REDACTED]
Such foreign intelligence information is particularly useful, for example, [REDACTED]
[REDACTED]

¹⁶ In

¹⁶ More specifically, during the course of the Court's consideration of DNI/AG-702(g) Certification [REDACTED] the Government explained the unique value of NSA's [REDACTED]

[REDACTED]

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

addition, NSA's upstream collection enables NSA to acquire foreign intelligence information from [REDACTED]

[REDACTED] All of these types of communications are intercepted in transactions acquired through NSA's upstream collection. Valuable foreign intelligence information such as this simply cannot be obtained by means other than the acquisition of transactions through NSA's upstream collection. ~~(TS//SI//NF)~~

3. The Acquisition of Foreign Intelligence Information Contained in Transactions is Conducted Using the Least Intrusive Means Available.
~~(TS//SI//NF)~~

The fact that NSA's upstream collection acquires transactions that may contain several discrete communications, only one of which is to, from, or about a tasked selector, does not render NSA's upstream collection unreasonable. *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); *see also United States v. Bin Laden*, 126 F. Supp. 2d 264, 280 (S.D.N.Y. 2000) ("[I]ncidental interception of a person's conversations during an otherwise lawful [Title III] surveillance is not violative of the Fourth Amendment."); *cf. 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"). Indeed, the Supreme Court has repeatedly rejected suggestions that reasonableness requires "the least intrusive search practicable." *City of Ontario v. Quon*, 130 S. Ct. 2619, 2632 (2010) (quotation marks omitted); *see, e.g., Earls*, 536 U.S. at 837 ("[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 quotation marks omitted)); *Vernonia*, 515 U.S. at 663 ("We have repeatedly refused to declare

[REDACTED]

~~(TS//SI//OC,NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment." (TS//SI//NF)

Although not demanded by the Fourth Amendment, NSA is nevertheless conducting "the least intrusive search practicable" when it acquires a single transaction which may contain several discrete communications, only one of which may contain foreign intelligence information because it is to, from, or about a tasked selector.

Accordingly, at the time of acquisition, NSA generally cannot know whether a transaction contains only a single communication to, from, or about a tasked selector, or whether that transaction contains that single communication along with several other communications.¹⁷

also render the information 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 contained within that discrete communication, therefore, is to acquire the entire transaction in which it is contained. 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. 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"). (TS//SI//NF)

At the same time, NSA is making every reasonable effort to ensure that its upstream collection acquires this singularly valuable foreign intelligence information in a manner that minimizes the intrusion into the personal privacy of United States persons to the greatest extent possible. As discussed above, these acquisitions are conducted in accordance with FISC-approved targeting procedures reasonably designed to ensure that the acquisitions are directed only "toward communications that are likely to yield the foreign intelligence information sought." Mem. Op. at 39-40 (footnote omitted). The application of the targeting procedures further ensures that "[t]he targeting of communications pursuant to Section 702 is designed in a manner that diminishes the likelihood that United States person information will be obtained." Mem. Op. at 23; cf. *In re Directives*, Docket No. 105B(g):07-01, Mem. Op. at 87 (USFISC April 25, 2008) (recognizing 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") (footnote omitted), *aff'd*, 551 F.3d 1004 (Foreign Int. Surv. Ct. Rev. 2008). Lastly, to the extent that United States person information is incidentally acquired in the acquisition of a whole transaction by NSA's upstream collection,

¹⁷ See Government's response to questions 2(c) and (d) *infra*. (U)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

such information will be handled in accordance with strict minimization procedures, as discussed in more detail below. ~~(TS//SI//NF)~~

4. United States Person Information Acquired Incidentally Through NSA's Acquisition of Transactions Containing Multiple Discrete Communications is Protected by NSA's Section 702 Minimization Procedures. ~~(TS//SI//NF)~~

As discussed above, the fact that NSA's upstream collection may result in the incidental acquisition of communications of United States persons cannot, by itself, render the overall collection unreasonable. Instead, courts have repeatedly found support for the constitutionality of foreign intelligence activities resulting in the incidental acquisition of United States person information in the existence and application of robust minimization procedures. See, e.g., *In re Directives*, 551 F.3d at 1015 (recognizing that minimization procedures are a "means of reducing the impact of incidental intrusions into the privacy of non-targeted United States persons");

~~Mem. Op. at 40 (concluding that minimization procedures meeting the definition in 50 U.S.C. § 1801(h)(1) "constitute a safeguard against improper use of information about United States persons that is inadvertently or incidentally acquired, and therefore contribute to the Court's overall assessment that the targeting and minimization procedures are consistent with the Fourth Amendment").~~ As explained below, NSA's current Section 702 minimization procedures, which this Court previously has found to satisfy the definition of minimization procedures in 50 U.S.C. § 1801(h)(1),¹⁸ adequately protect the privacy interests of United States persons whose communications may be incidentally acquired through NSA's upstream collection and thus contribute significantly to the overall reasonableness of that collection. ~~(TS//SI//NF)~~

At the outset, it is worth noting that NSA's acquisition of Internet transactions containing multiple discrete communications does not necessarily increase the risk that NSA will incidentally acquire United States person information. For example, as discussed above, the ~~means by which NSA ensures it does not intentionally acquire wholly domestic communications limits the acquisition of certain transactions such as~~ to persons located outside the United States, who reasonably can be presumed to be non-United States persons. Thus, to the extent that the ~~of those non-United States persons contain communications that are not to, from, or about a targeted selector, those communications are unlikely to be United States person communications.~~ See *In re Directives*, Docket No. 105B(g):07-01, Mem. Op. at 87 (recognizing 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") (footnote omitted). For this same reason, the risk that United States person information would be obtained through the acquisition of a ~~is no greater than in the acquisition of a~~

¹⁸ 50 U.S.C. § 1801(h)(1) defines "minimization procedures" as "specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, 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." (U)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~~~(TS//SI//NF)~~

a. Acquisition (U)

As discussed above, with limited exceptions,¹⁹ it is technologically infeasible for NSA's upstream collection to acquire only the discrete communication to, from, or about a tasked selector that may be contained in a transaction containing multiple discrete communications. That does not mean, however, that the minimization procedures governing NSA's upstream collection do not adequately minimize the acquisition of any United States person information that may be contained in those transactions. Specifically, minimization procedures must be reasonably designed to minimize the acquisition 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." 50 U.S.C. § 1801(h)(1). As discussed above, the *only* way to obtain the foreign intelligence information contained within a discrete communication is to acquire the entire transaction in which it is contained. Thus, to the extent that United States person information may be contained within other discrete communications not to, from, or about the target in that transaction, the acquisition of such United States person information would be "consistent with the need of the United States to obtain . . . foreign intelligence information." ~~(TS//SI//NF)~~

Congress has recognized that "in many cases it may not be possible for technical reasons to avoid acquiring all information" when conducting foreign intelligence surveillance. H.R. Rep. No. 95-1283, pt. 1, at 55 (1978); *see also id.* at 56 ("It may not be possible or reasonable to avoid acquiring all conversations."); *cf. Scott*, 436 U.S. at 140 (recognizing that Title III "does not forbid the interception of all nonrelevant conversations, but rather instructs the agents to conduct the surveillance in such a manner as to 'minimize' the interception of such conversations"). Rather, in situations where, as here, it is technologically infeasible to avoid incidentally acquiring communications that are not to, from, or about the target, "the reasonable design of the [minimization] procedures must emphasize the minimization of retention and dissemination." H.R. Rep. No. 95-1283, pt. 1, at 55. ~~(TS//SI//NF)~~

b. Retention (U)

In addition, for reasons discussed more fully below, nothing in the statutory definition of minimization procedures obligates NSA to immediately destroy any United States person information in a communication that is not to, from, or about a tasked selector within a transaction acquired by NSA's upstream collection. ~~(TS//SI//NF)~~

¹⁹ See *supra* footnote 6. (U)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~**i. Destruction Is Not Technologically Feasible** ~~(TS//SI//NF)~~

First, Congress intended that the obligation to destroy non-pertinent information would attach only if the destruction of such information is 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)). That is because Congress recognized that in some cases, the 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 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."). ~~(TS//SI//NF)~~

A transaction containing several communications, only one of which contains the tasked selector, is to NSA's systems technologically indistinguishable from a transaction containing a single message to, from, or about a tasked selector. That is true both for NSA's collection systems and for the NSA systems that process and then route Section 702-acquired information to NSA's corporate stores. Thus, unlike other instances where it is technologically possible for certain kinds of communications to be recognized, segregated, and prevented from being routed to NSA's corporate stores, the transaction as a whole, including all of the discrete communications that may be included within it, is forwarded to NSA corporate stores, where it is available to NSA analysts. ~~(TS//SI//NF)~~

The transaction is likewise not divisible into the discrete communications within it even once it resides in an NSA corporate store. That is because NSA assesses that it is not technologically feasible to extract, post-acquisition, only the discrete communication that is to, from, or about a tasked selector within a transaction without destabilizing -- and potentially rendering unusable -- some or all of the collected transaction, including the single, discrete communication which is to, from or about the tasked selector. Thus, an NSA analyst cannot, for example, simply cut out any pertinent part of the transaction (i.e., the discrete communication that contains the tasked selector), paste it into a new record, and then discard the remainder. In this way, the transactions at issue here are a present-day version of the very same problem that Congress recognized over thirty years earlier -- i.e., that in some cases, "it might not be feasible to cut and paste files . . . where some information is relevant and some is not." H.R. Rep No. 95-1283, pt.1, at 56. Given that Congress recognized it might be necessary to retain all acquired information regardless of its pertinence because destruction of the non-pertinent information may not be feasible, minimization procedures that permit the retention of transactions in their entireties because their further divisibility is infeasible (if not technologically impossible) are consistent with the statutory requirement that such procedures minimize the retention of United States person information. ~~(TS//SI//NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

ii. **Retention of United States Person Information Can Be Effectively Minimized Through Restrictions on its Retrieval** ~~(TS//SI//NF)~~

Second, although it is not required that all non-pertinent United States person information be destroyed, NSA's retention of non-pertinent information concerning innocent United States persons is not without bounds. FISA's legislative history suggests that the retention of such information could still be effectively minimized through means other than destruction. *See* H.R. Rep. No. 95-1283, pt. 1, at 56 ("There are a number of means and techniques which the minimization procedures may require to achieve the purposes set out in the definition."). Of particular relevance here, Congress recognized that minimizing the retention of such information can be accomplished by making the information "not retrievable by the name of the innocent person" through the application of "rigorous and strict controls." *Id.* at 58-59. Those "rigorous and strict controls," however, need only be applied to the retention of United States person information "for purposes other than counterintelligence or counterterrorism." *Id.* That is because Congress intended that "a significant degree of latitude be given in counterintelligence and counterterrorism cases with respect to the retention of information." *Id.* at 59. ~~(TS//SI//NF)~~

NSA's current Section 702 minimization procedures flatly prohibit the use of United States person names or identifiers to retrieve any Section 702-acquired communications in NSA systems. *See, e.g.,* Amendment 1 to DNI/AG 702(g) Certification [REDACTED] Ex. B, filed [REDACTED] 2010, § 3(b)(5) (hereinafter "NSA Section 702 minimization procedures"). This "rigorous and strict control[]" applies even to United States person information that relates to counterintelligence or counterterrorism, despite Congress's stated intent that agencies should have "a significant degree of latitude . . . with respect to the retention of [such] information." H.R. Rep. No. 95-1283, pt. 1, at 59; *see id.* at 58-59 (recognizing that "for an extended period it may be necessary to have information concerning [the] acquaintances [of a hypothetical FISA target] retrievable" for analytic purposes, even though "[a]mong his contacts and acquaintances . . . there are likely to be a large number of innocent persons"). NSA's current Section 702 minimization procedures thus require the retention of information concerning United States persons (innocent or otherwise) to be minimized to a significantly greater degree than is necessary for those procedures to be reasonable. ~~(TS//SI//NF)~~

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. *E.g.,* DNI/AG 702(g) Certification [REDACTED] Ex. B, filed Apr. 20, 2011, § 3(b)(5). Under these revised NSA Section 702 minimization procedures, the use of such selection terms must be approved in accordance with NSA procedures. *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. The Government will ensure that these NSA procedures contain "rigorous and strict controls" on the retrieval of United States person information consistent with statutory requirements and Congressional intent. H.R. Rep. No. 95-1283, pt. 1, at 59. ~~(TS//SI//NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

c. Dissemination (U)

As discussed above, the NSA current Section 702 minimization procedures prohibit the use of United States person identifiers to retrieve any Section 702-acquired communications in NSA systems. Accordingly, the only way incidentally acquired United States person information currently will be reviewed by an NSA analyst is if that information appears in a communication that the analyst has retrieved using a permissible query term -- i.e., one that is reasonably likely to return information about non-United States person foreign intelligence targets. See NSA Section 702 minimization procedures, § 3(b)(5). Any identifiable United States person information contained in a communication retrieved in this manner would be subject to the dissemination restrictions in the NSA Section 702 minimization procedures, which operate to ensure that any dissemination of United States person information is consistent with the Act. These restrictions apply regardless of whether the United States person information is contained in a discrete communication that is to, from, or about a tasked selector. Moreover, the same dissemination restrictions will continue to apply to any United States person information retrieved through the use of a United States person identifier as a selection term in accordance with NSA's revised 702 minimization procedures. Indeed, given the small probability that an incidentally acquired communication of a United States person that is not to, from, or about a tasked selector would contain foreign intelligence information or evidence of a crime, it is highly unlikely that NSA would disseminate any information from that incidentally acquired communication, let alone information concerning the United States person. (TS//SI//NF)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~



20 [Redacted] ~~(TS//SI//NF)~~

21 [Redacted] ~~(TS//SI//NF)~~

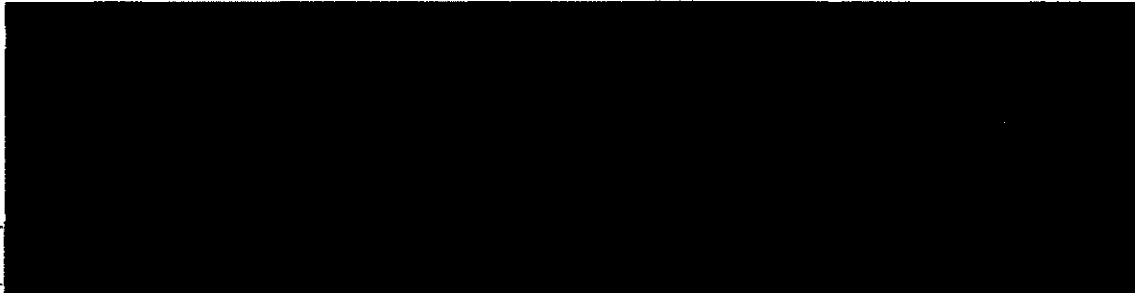
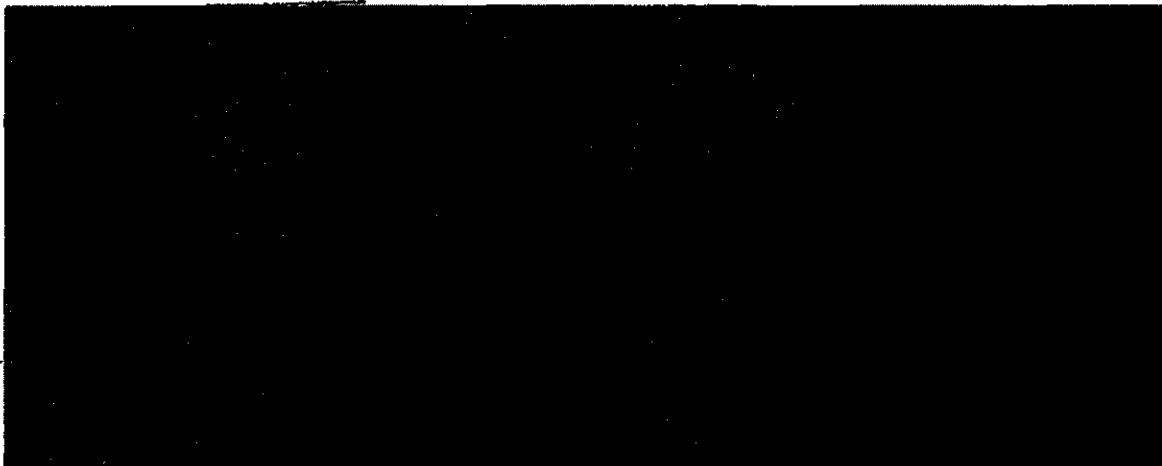
²² See footnote 22 below. (S)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~



c. The May 2 Letter states that NSA is not presently capable of "separating out individual pieces of information" contained within [redacted] May 2 Letter at 3. Please explain why and state whether it would be feasible for NSA to implement such capability, either at the time of acquisition or thereafter. ~~(TS//SI//NF)~~

d. Can [redacted] be identified as distinct from other, discrete communications between users, either at the time of acquisition or thereafter? If so, can NSA filter its Section 702 collection on this basis? ~~(TS//SI//NF)~~



Except as described above, at the time of acquisition, NSA is not presently capable of separating out transactions that contain multiple electronic communications into logical constituent parts without destabilizing -- and potentially rendering unusable -- some or all of the entire collected transaction, including any particular communication therein which is in fact to, from, or about the tasked selector. Each electronic communication service provider develops protocols that perform the services being provided in a manner designed to be economical in speed, size, and other factors that the provider considers important. [redacted]

²⁵ An NSA analyst would, however, 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, such as an analytic store. Even so, the original transaction from which that copy was made would be retained in the corporate store in its original state, which cannot be altered for the reasons discussed below. ~~(TS//SI//NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Each of the major providers change protocols often to suit their own business purposes, and it is therefore generally not possible for NSA to isolate or separate out individual pieces of information contained within single transactions at the time of NSA acquisition. Any protocol in use today could easily be changed by the provider tomorrow [REDACTED]

[REDACTED]

In short, except in cases involving [REDACTED] described above, at the time of acquisition it is not technologically feasible for NSA to extract any particular communication that is to, from, or about a tasked selector within a transaction containing multiple discrete communications. (TS//SI//NF)

For the same reasons that protocol volatility and myriad user settings prevent the extraction of only discrete communications at the point of acquisition, it is not technologically feasible to extract, post-acquisition, only the specific communication(s) to, from, or about a tasked selector within a transaction without destabilizing -- and potentially rendering unusable -- some or all of the collected transaction, including any particular communication therein which is to, from, or about the tasked selector. Thus, an NSA analyst cannot, for example, simply cut out the discrete communication that contains the tasked selector, paste it into a new record, and then discard the remainder. (TS//SI//NF)

3. The May 2 Letter notes that NSA uses Internet Protocol (IP) filtering and [REDACTED] to prevent the intentional acquisition of communications as to which the sender and all known recipients are inside the United States. May 2 Letter at 3. (TS//SI//NF)

a. Please describe how NSA applies IP filtering in the context of [REDACTED] (TS//SI//NF)

i. [REDACTED] (TS//SI//NF)

ii. [REDACTED] (TS//SI//NF)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

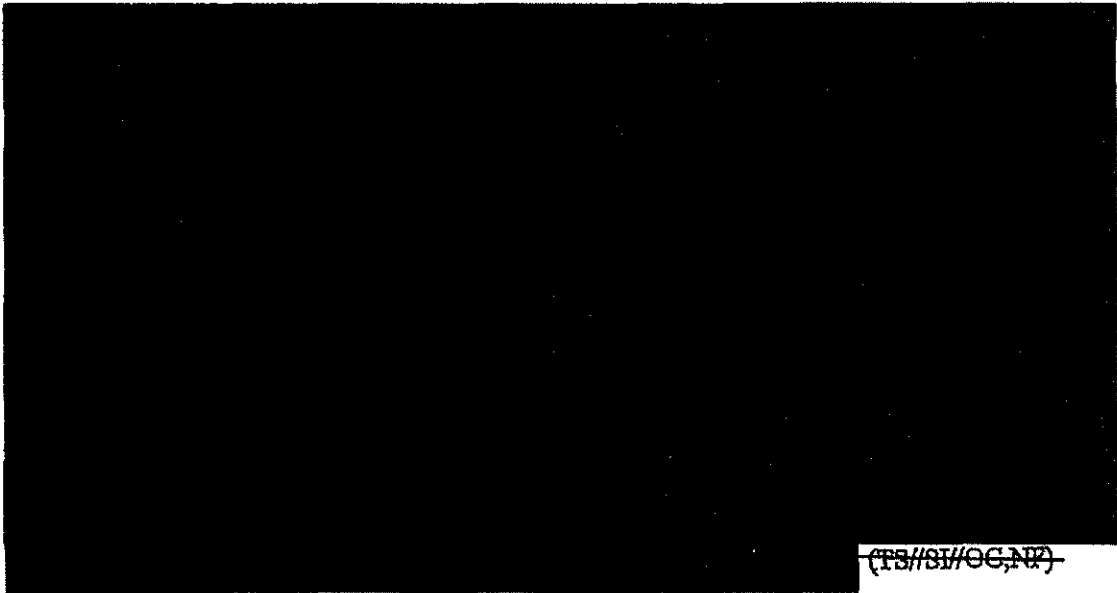
All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

NSA acquires Internet communications by collecting the individual packets of data that make up those communications. As required by NSA's targeting procedures, all Internet communications data packets that may contain abouts information that NSA intercepts through its Section 702 upstream collection must either pass through an "Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas." or



~~(TS//SI//OC,NF)~~



~~(TS//SI//OC,NF)~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

[REDACTED] Accordingly, NSA cannot prevent the acquisition of, or even mark for separate treatment, those types of transactions that may feature multiple discrete communications [REDACTED] (TS//SI//OC,NF)

- b. In the collection of "to/from" communications, are the communicants always the individual users of particular facilities [REDACTED], or does NSA sometimes consider [REDACTED] Please explain. (TS//SI//NF)

In the collection of "to/from" communications, NSA considers the communicants as being the individual users of particular selectors. More particularly, NSA considers those individual users to be the senders and intended recipients of "to/from" communications. Conversely, NSA does not consider [REDACTED] (TS//SI//NF)

- 4. How, in terms of numbers and volume, does NSA's collection of [REDACTED] under Section 702 compare with the collection of discrete Internet communications (such as e-mail messages) between or among individual users? (TS//SI//NF)

As a result of the present technological limitations [REDACTED] NSA cannot precisely measure the number of transactions that might contain information or data representing several discrete communications [REDACTED] for purposes of comparing that figure with transactions containing a single, discrete communication [REDACTED] without manually examining each transaction that NSA has acquired. However, in an attempt to provide an estimate of the volume of such collection at the Court's request, NSA performed a series of queries into the SIGINT Collection Source System of Record that holds the relevant transactions in question. [REDACTED]

Results were sampled manually to confirm collection of [REDACTED] 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]²⁶ It is important

²⁶ NSA notes that it is likely that this 9% figure includes [REDACTED] of the user of the targeted selector him/herself. (TS//SI//NF)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

to note that this was a manually intensive and imprecise means to quantify the volume of [REDACTED] collection and should not be interpreted to suggest that any technological method of pre-filtering can be applied to the collection before it is available to the analyst. ~~(TS//SI//NF)~~

5. Given that some of the information acquired through upstream collection is likely to constitute "electronic surveillance" as defined in 50 U.S.C. § 1801(f)(2) that has not been approved by this Court, how does the continued acquisition of, or the further use or dissemination of, such information comport with the restrictions of 50 U.S.C. § 1809(a)(1) and (a)(2)? ~~(TS//SI//NF)~~
- I. **THE CONTINUED ACQUISITION, USE, AND DISSEMINATION OF INFORMATION ACQUIRED THROUGH UPSTREAM COLLECTION DOES NOT VIOLATE 50 U.S.C. § 1809.** ~~(TS//SI//NF)~~

A. Introduction (U)

Section 702 of FISA, as codified at 50 U.S.C. § 1881a, provides that "[n]otwithstanding any other provision of law," upon the issuance of an appropriate Order from the Court, the Attorney General (AG) and the Director of National Intelligence (DNI) may jointly authorize the targeting of non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information as long as certain conditions set out in subsection 702(b) are met. The joint authorizations of the AG and the DNI authorized NSA's upstream acquisition of communications that are to, from, or about a tasked selector. The Court, in turn, approved the implementing certifications as well as the use of proffered targeting and minimization procedures. Accordingly, because the acquisition of communications to, from, or about a tasked selector was authorized by the AG and DNI, and the Court approved the certifications and procedures used to implement those authorizations, NSA's acquisition of such communications upstream does not constitute unauthorized electronic surveillance and, therefore, does not violate the terms of 50 U.S.C. § 1809. ~~(TS//SI//NF)~~

As noted above, the Government readily acknowledges that it did not fully describe to the Court that the upstream collection technique would result in NSA acquiring [REDACTED] types of Internet transactions that could include multiple individual, discrete communications [REDACTED]. As discussed below, however, this omission does not invalidate the AG and DNI's prior authorizations. Nor does it mean that the incidental acquisition of communications that are not to, from, or about a tasked selector as a consequence of obtaining communications that are to or from a tasked selector or contain reference to a tasked selector, exceeds the scope of those authorizations. For the same reasons, the Government respectfully suggests that the Orders of

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

this Court upon which those authorizations rely likewise remain valid. Thus, Section 1809 is not implicated by NSA's upstream collection activities under Section 702. ~~(TS//SI//NF)~~

B. Statutory Framework (U)

i. Section 1809 (U)

Under Subsection 1809(a), a person is guilty of a criminal offense if he or she "intentionally (1) engages in electronic surveillance under color of law, except as authorized by this Act . . . ; or (2) disclose[s] 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 this Act."²⁷ (U)

For purposes of Section 1809 the issue is whether the Government's prior failure to fully explain to the Court the steps NSA must take in order acquire communications to, from, or about a tasked selector, and certain technical limitations regarding the IP address filtering it applies, means that the acquisition of such communications was not authorized by the DNI and AG, and inconsistent with Court approval of the targeting and minimization procedures. ~~(TS//SI//NF)~~

ii. Section 702 Collection Authorizations ~~(S)~~

Pursuant to 50 U.S.C. § 1881a(a), "notwithstanding any other provision of law," the AG and the DNI may jointly authorize for a period of up to one year the targeting of non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information, subject to targeting and minimization procedures approved by this Court, and certain limitations set out in § 1881a(b). Authorizations are premised on certifications to the Court, in which the AG and DNI attest to the fact that, among other things, the targeting and minimization procedures comply with certain statutory requirements and the Fourth

²⁷ This Court has previously noted that the legislative history of this provision focuses on a predecessor bill that was substantially different from the provision subsequently enacted and codified. ~~See [REDACTED]~~ Mem. Op. at 6-7 (Dec. 10, 2010). Yet, both the predecessor bill and the codified provision use the word intentionally, which has been described as "carefully chosen" and intended to limit criminal culpability to those who act with a "conscious objective or desire" to commit a violation. See H.R. Rep. No. 95-1283, pt.1, at 97 (1978) ("The word 'intentionally' was carefully chosen. It is intended to reflect the most strict standard for criminal culpability. . . . The Government would have to prove beyond a reasonable doubt both that the conduct engaged in was in fact a violation, and that it was engaged in with a conscious objective or desire to commit a violation."). Based upon discussions between responsible NSA officials and the Department of Justice (DOJ) and the Office of the Director of National Intelligence (ODNI) and DOJ and ODNI's review of documents related to this matter, DOJ and ONDNI have not found any indication that there was a conscious objective or desire to violate the authorizations here. ~~(TS//SI//NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Amendment. 50 U.S.C. § 1881a(g)(2). Authorizations become effective “upon the issuance of an order [of this Court]” approving the certification and the use of the targeting and minimization procedures as consistent with the statute and the Fourth Amendment. *Id.* §§ 1881a(a) (AG and DNI authorizations go into effect upon “issuance of an order”); 1881a(i)(2)-(3) (laying out scope of FISC review).²⁸ ~~(TS//SI//NF)~~

Thus, if an acquisition is authorized by the AG and DNI, and the certification and targeting and minimization procedures which implement that authorization are approved by the Court, and the authorization remains valid, then the acquisition does not constitute unauthorized electronic surveillance under 50 U.S.C. § 1801(f)(2) and is not a violation of 50 U.S.C. § 1809. ~~(TS//SI//NF)~~

C. At a Minimum, the Upstream Acquisition of Single, Discrete Communications To, From, or About a Tasked Selector Was Authorized by the AG and the DNI

~~(TS//SI//NF)~~

The relevant AG and DNI authorizations and the targeting procedures the AG approved explicitly permit the acquisition of Internet communications that are to, from, or about a tasked selector. *See, e.g.*, NSA Targeting Procedures at 1 (describing the safeguards used in the acquisition of “about” as compared with “to/from” communications). In addition, the accompanying Affidavits of the Director of NSA described upstream collection in a paragraph detailing the various methods of obtaining such acquisitions. *See, e.g.*, DNI/AG 702(g) Certification [REDACTED] Affidavit of General Keith B. Alexander, Director, NSA, filed July 16, 2010, ¶ 4. Thus, it is clear that the authorizations permit – at a minimum – the upstream acquisition of single, discrete communications to, from, or about a tasked selector. ~~(TS//SI//NF)~~

As described in detail in response to questions 2 and 3 above, due to certain technological limitations, in general the only way NSA can currently acquire as part of its upstream collection single, discrete communications to, from, or about a tasked selector [REDACTED] is by obtaining the Internet transactions of which those communications are a part. An Internet transaction can include either a single, discrete communication to, from, or about a tasked

²⁸ For reauthorizations, the AG and the DNI submit, to the extent possible, a certification to the FISC laying out, among other things, the targeting and minimization procedures adopted at least 30 days prior to the expiration of the prior authorization. The prior authorization remains in effect, notwithstanding the otherwise applicable expiration date, pending the FISC's issuance of an order with respect to the certification for reauthorization. 50 U.S.C. § 1881a(i)(5). The scope of the court's review is the same for reauthorizations as it is for initial authorizations. *Id.* § 1881a(i)(5)(B). (U)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

selector [REDACTED], or several discrete communications, only one of which may be to, from, or about a tasked selector [REDACTED] ~~(TS//SI//NF)~~

Where an Internet transaction includes multiple communications, not all of which are to, from, or about a tasked selector, it currently may not be technologically feasible for NSA to separate out, at the time of acquisition or thereafter, the discrete electronic communications within that transaction that are to, from, or about a tasked selector. Indeed, at the time of acquisition, NSA's upstream Internet collection devices are, with limited exception, not capable of distinguishing or further separating discrete electronic communications [REDACTED] within a single Internet transaction. Thus, in some cases, NSA can collect communications to, from, or about a tasked selector, as authorized by the certification, only by obtaining the Internet transaction of which those communications may be just a part.

~~(TS//SI//NF)~~

In this respect, the upstream acquisition of Internet transactions which contain multiple, discrete communications not all of which are (and, in some instances, only one of which is) to, from or about a tasked selector is akin to the Government's seizure of a book or intact file that contains a single page or document that a search warrant authorizes the government to seize. In *United States v. Wuagneux*, 683 F.2d 1343, for example, the Eleventh Circuit rejected appellants' argument that a search was unreasonable because the agents seized an entire file, book, or binder if they identified a single document within the file, book, or binder as being within the authorization of the warrant. As the court explained, "a search may be as extensive as reasonably required to locate items described in the warrant." *Id.* at 1352. It was therefore "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." *Id.* at 1353. *See also 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); *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"). ~~(TS//SI//NF)~~

That the certifications by the AG and DNI did not specifically describe this aspect of NSA's upstream collection does not mean that collection was unauthorized by the AG and DNI. Again, case law involving the reasonableness of searches conducted pursuant to criminal search warrants is instructive on this point. For example, in *Dalia v. United States*, 441 U.S. 238, 259 (1979), the Supreme Court recognized that "[o]ften in executing a warrant the police may find it

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

necessary to interfere with privacy rights not explicitly considered by the judge who issued the warrant." *Id.* at 257. 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.") (quoting *Dalia*, 441 U.S. 238, 257 (1979)). This is especially true where, as in *Dalia*, "[t]here is no indication that [the] intrusion went beyond what was necessary" to effectuate the search authorized. *Dalia*, 441 U.S. at 258 n. 20. ~~(TS//SI//NF)~~

Like the seizure of an entire book or file simply because it contained a single page or document within the scope of the warrant, NSA only acquires an Internet transaction containing several discrete communications if at least one of those communications within the transaction is to, from, or about a tasked selector. Moreover, unlike the agents in *Wuagneux*, who presumably could have opted to seize only the responsive pages out of the books and files searched, except in limited circumstances, NSA has no choice but to acquire the whole Internet transaction in order to acquire the to, from, or about communication the DNI and AG authorized NSA to collect. NSA only acquires an Internet transaction if *in fact* it contains at least one communication to, from, or about a tasked selector. NSA's acquisition of Internet transactions containing several discrete communications, only one of which is to, from, or about a tasked selector, is therefore "as extensive as reasonably required to locate the items described" in the DNI and AG's authorization, and thus cannot be said to exceed the scope of that authorization. ~~(TS//SI//NF)~~

Moreover, as described in response to questions 1(b)(ii) and (iii), the Government has concluded that such collection fully complies with the statutory requirements and the Fourth Amendment. Having now considered the additional information that is being presented to this Court, the AG and DNI have confirmed that their prior authorizations remain valid. Accordingly, Government personnel who rely on those authorizations to engage in ongoing acquisition are not engaging in unauthorized electronic surveillance, much less doing so "intentionally." ~~(TS//SI//NF)~~

D. The Court Approved the Certifications and Targeting and Minimization Procedures Used to Implement the Authorizations of the AG and DNI ~~(TS//SI//NF)~~

A second issue concerns whether this Court's orders cover the full scope of the authorizations, and, if not, whether that affects the validity of the AG and DNI authorizations. Like the AG and DNI authorizations, in approving the applicable certifications and the use of the proffered targeting and minimization procedures this Court's Opinions and Orders clearly contemplated and approved some upstream collection of communications to, from, or about a target. See, e.g., [REDACTED] Mem. Op. at 15-17 (describing acquisition of communications to, from,

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

and about a target).²⁹ Thus, for the reasons described above, the acquisition of Internet transactions that include at least one communication to, from, or about a target falls within the scope of the Court's Orders – even if additional communications are also incidentally acquired due to limits in technology. ~~(TS//SI//NF)~~

The fact that the Government did not fully explain to the Court all of the means by which such communications are acquired through NSA's upstream collection techniques does not mean that such acquisitions are beyond the scope of the Court's approval, just as in the criminal context a search does not exceed the scope of a warrant because the Government did not explain to the issuing court all of the possible means of execution, even when they are known beforehand and could possibly implicate privacy rights. See *Dalia*, 441 U.S. at 257 n.19 (noting that "[n]othing in the decisions of this Court . . . indicates that officers requesting a warrant should be constitutionally required to set forth the anticipated means for execution even in those cases where they know beforehand that [an additional intrusion such as] unannounced or forced entry likely will be necessary."). In addition, as discussed herein, the incidental acquisitions do not go beyond what is reasonably necessary to acquire the foreign intelligence information contained in a communication to, from, or about a targeted selector within a transaction. See *id.* at 258 n. 20. ~~(TS//SI//NF)~~

In any event, the Government believes that the additional information should not alter the Court's ultimate conclusion that the targeting and minimization procedures previously approved are consistent with the statutory requirements, including all the requirements of § 1881a(b), and the Fourth Amendment, and the Court's orders therefore remain valid. Cf. *Franks v. Delaware*, 438 U.S. 154 (1978) (establishing that a search warrant is valid unless it was obtained as the result of a knowing and intentional false statement or reckless disregard for the truth and the remaining content is insufficient to establish the requisite probable cause needed to obtain the warrant). ~~(TS//SI//NF)~~

Pursuant to § 1881a, the Court reviews the following issues: (i) whether the AG and DNI certifications contain all the required elements; (ii) whether the targeting procedures are consistent with the requirements of § 1881a(d)(1); (iii) whether the minimization procedures are consistent with § 1881a(i)(e)(1); and (iv) whether the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment. 50 U.S.C. § 1881a(i)(2), (3). See also *id.* § 1881a(i)(5)(B) (specifying that reauthorizations are to be reviewed under the same

²⁹ Each of the relevant 2010 FISC Orders is based on the "reasons stated in the Memorandum Opinion issued contemporaneously herewith." These Opinions, in turn, rely on the analysis conducted by the Court in Dockets [REDACTED], which incorporate and rely on the analysis of earlier FISC Opinions, including Docket 702(i)-08-01. ~~(TS//SI//NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

standards). The Government believes that the Court's ultimate conclusions with respect to each of these issues should not change based on the additional information provided. ~~(TS//SI//NF)~~

First, there is no suggestion that the prior certifications failed to contain all the required elements. ~~(TS//SI//NF)~~

Second, while the Government acknowledges that it did not fully explain to the Court the steps NSA must take in order to implement its Section 702 upstream Internet collection techniques, and certain technical limitations regarding its IP address filtering, the Court did approve the DNI/AG certifications and the use of targeting and minimization procedures which authorized the acquisition of communications to, from, or about tasked selectors. As discussed above and in response to questions 1(b)(ii) (iii) and 3, Internet transactions are collected because they contain at least one discrete communication to, from, or about a tasked selector. Each tasked selector has undergone review, prior to tasking, designed to ensure that the user is a non-United States person reasonably believe to be located outside the United States. Moreover, with respect to "abouts" communications, for the reasons discussed in the response to question 1(b)(ii), NSA's targeting procedures are reasonably designed to prevent the intentional acquisition of any communications as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States.³⁰ Thus, NSA is targeting persons reasonably believed to be outside the United States and is not intentionally acquiring communications in which both the sender and all intended recipients are known at the time of acquisition to be in the United States. ~~(TS//SI//NF)~~

Third, as described throughout, in many cases, it is not technologically feasible for NSA to acquire only Internet transactions that contain a single, discrete communication to, from, or about a tasked selector that may be contained in an Internet communication containing multiple discrete [REDACTED] communications. As discussed in detail in response to questions 1(b)(ii) and (iii), this does not mean that NSA's procedures do not adequately minimize the acquisition of any U.S. person information that may be contained within those transmissions. Rather, the minimization procedures fully comport with all statutory requirements. ~~(TS//SI//NF)~~

³⁰ As the Court is aware, § 1881a(b)(4) provides that an acquisition authorized under section 702, "may not intentionally acquire 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 . . ." Although this prohibition could be read at first glance to be absolute, another provision of Section 702 indicates otherwise. Specifically, § 1881a(d)(1)(B) provides that the targeting procedures that the AG, in consultation with the DNI, must adopt in connection with an acquisition authorized under section 702 need only be "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 in the United States." (U)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Finally, as described in response to question 1(b)(iii), the targeting and minimization procedures fully comply with the Fourth Amendment. ~~(TS//SI//NF)~~

Thus, the additional information the Government has provided concerning details of its upstream collection does not – in the Government's view – undercut the validity of the targeting or minimization procedures. ~~(TS//SI//NF)~~

E. Compliance with the Authorizations: Use and Disclosure ~~(TS//SI//NF)~~

As described above, § 1809(a)(2) criminalizes the intentional use and disclosure of electronic surveillance, "knowing or having reason to know that the information was obtained through electronic surveillance not authorized by this Act." Having concluded that the upstream collection conducted by NSA falls within the scope of the relevant authorizations, the Government respectfully submits that the continued use and disclosure of such information is likewise valid, so long as the minimization procedures approved by the Court (and discussed in detail in response to questions 1(b)(ii) and (iii)) are followed.³¹ ~~(TS//SI//NF)~~

6. Please provide an update regarding the [REDACTED] over collection incidents described in the government's letter to the Court dated April 19, 2011.

The April 19, 2011, notice to the Court described two overcollection incidents involving entirely unrelated communications that had been [REDACTED]. The notice also advised that as part of its continued investigation into these incidents, NSA would examine other systems to determine whether similar [REDACTED] issues occurred in those systems. ~~(TS//SI//NF)~~

The first incident described in the April 19 notice involved [REDACTED]. Each [REDACTED] contained at least one communication to, from, or about a Section 702-tasked selector, but also [REDACTED] unrelated communications. This overcollection started [REDACTED].

³¹ Although this analysis has focused on acquisitions conducted pursuant to the 2010 Section 1881a Authorizations, the Government believes that, for all of the reasons discussed herein, the upstream collection conducted pursuant to previous certifications authorized under Section 1881a of the Foreign Intelligence Surveillance Act of 1978, as amended, the Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (Aug. 5, 2007), [REDACTED]

[REDACTED] falls within the scope of the relevant authorizations and Orders of this Court.

~~(TS//SI//NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

[REDACTED] (S//SI//NF)

[REDACTED]

All such communications will be processed in accordance with NSA's minimization procedures.³² The Government will advise the Court of the final disposition of these communications.

[REDACTED] (S//SI//NF)

The second-described [REDACTED] incident involved overcollection [REDACTED]. As described in the April 19 notice, on March 28, 2011, NSA discovered a [REDACTED] of Section 702-acquired communications that had not been properly [REDACTED]

In contrast to the [REDACTED] communications overcollected between [REDACTED] discussed above, the [REDACTED] acquired as a result of the [REDACTED] overcollection incident involved fewer communications [REDACTED]

³² In particular, section 3(b)(1) of NSA's Section 702 Minimization Procedures state:

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 in the processing cycle 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. Such inadvertently acquired communications of or concerning a United States person may be retained no longer than five years in any event. The communications that may be retained include electronic communications acquired because of limitations on NSA's ability to filter communications.

(Emphasis added). (S//SI)

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

As in the [redacted] incident, each [redacted] contains at least one communication that is to, from, or about a Section 702-task selector. (TS//SI//NF)

As of April 11, 2011, NSA began to sequester in its Collection Stores all communications involving the affected [redacted]

[redacted]. NSA was deliberately overinclusive in adding objects to the [redacted]; while some of these objects include [redacted] other objects consist of only one communication to, from, or about a Section 702-task selector.

~~(TS//SI//NF)~~

Since the filing of the April 19 notice, NSA has continued to evaluate collection from [redacted] and has observed no evidence of [redacted] issues other than the above-described issues [redacted]

~~(TS//SI//NF)~~

NSA has identified no reporting based upon overcollected communications and is currently exploring options to automate ways to accelerate identification of [redacted]

[redacted] NSA anticipates that it will be able to reach a decision by June 30, 2011, on whether this approach is effective. ~~(TS//SI//NF)~~

~~(TS//SI//NF)~~

The April 19 notice also advised the Court that NSA would "examine [redacted] and other upstream collection systems to ensure that similar [redacted] problems are not occurring in those systems." NSA now reports that unlike the most recent [redacted]

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//ORCON,NOFORN~~

these other systems were designed [redacted] ³³ [redacted]
[redacted]
[redacted] ~~(S//SI//NF)~~

7. Are there any other issues of additional information that should be brought to the Court's attention while it is considering the certifications and amendments filed in the above-captioned dockets?

At this time, the Department of Justice (DOJ) and Office of the Director of National Intelligence (ODNI) are currently investigating certain possible incidents of non-compliance about which the Department of Justice intends to file preliminary notices in accordance with the rule of this Court. These incidents do not relate to any of the matters discussed in this filing and, based on the information currently available to DOJ and ODNI, the Government does not believe that the nature of these incidents is sufficiently serious such that they would bear on the Court's consideration of the certifications and amendments filed in the above-captioned dockets.

~~(S//OC,NF)~~

³³ As discussed in response to question 2(c) and (d), NSA has the ability to separate out individual pieces of information in certain cases [redacted] In the course of the investigation into the most recent [redacted] incident, NSA additionally identified [redacted]

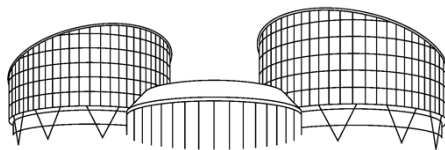
[redacted] Though testing demonstrated the possibility that incompletely processed communications could have been forwarded through the SIGINT system, NSA has identified no actual overcollection that occurred as a result. NSA is currently in the process of developing a software fix designed to properly process such communications under the limited circumstances in which overcollections could occur. Until such a fix can be tested and deployed, NSA will continue to monitor [redacted] and other upstream Section 702 collection systems [redacted]

~~(S//SI//NF)~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 23



EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

FIRST SECTION

**CASE OF BIG BROTHER WATCH AND OTHERS
v. THE UNITED KINGDOM**

(Applications nos. 58170/13, 62322/14 and 24960/15)

JUDGMENT

STRASBOURG

13 September 2018

Request for referral to the Grand Chamber pending

This judgment will become final in the circumstances set out in Article 44 § 2 of the Convention. It may be subject to editorial revision.



JA2933

BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

TABLE OF CONTENTS

PROCEDURE1

THE FACTS2

I. THE CIRCUMSTANCES OF THE CASE.....2

 A. Background2

 B. The secret surveillance schemes3

 1. Government Communications Headquarters (“GCHQ”)3

 2. The United States’ National Security Agency (“NSA”).....4

 (a) PRISM4

 (b) Upstream4

 C. Domestic proceedings in the first and second of the joined cases5

 D. Domestic proceedings in the third of the joined cases.....5

 1. The hearing6

 2. The IPT’s first judgment of 5 December 2014.....8

 (a) The PRISM issue8

 (b) The section 8(4) issue.....11

 3. The IPT’s second judgment of 6 February 201514

 4. The IPT’s third judgment of 22 June 2015 as amended by its 1 July 2015
 letter15

II. RELEVANT DOMESTIC LAW AND PRACTICE16

 A. The interception of communications16

 1. Warrants: general.....16

 2. Warrants: section 8(4).....18

 (a) Authorisation18

 (b) “External” communications18

 3. Specific safeguards under RIPA.....19

 (a) Section 1519

 (b) Section 16.....20

 4. The Interception of Communications Code of Practice22

 5. Statement of Charles Farr35

 6. Belhadj and Others v. Security Service, Secret Intelligence Service,
 Government Communications Headquarters, the Secretary of State for
 the Home Department, and the Secretary of State for the Foreign and
 Commonwealth Office, IPT/13/132-9/H and IPT/14/86/CH.....35

 B. Intelligence sharing36

 1. British-US Communication Intelligence Agreement.....36

 2. Relevant statutory framework for the operation of the intelligence
 services.....36

 (a) MI537

 (b) MI6.....37

BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

(c) GCHQ.....	37
(d) Counter-Terrorism Act 2008.....	38
(e) The Data Protection Act 1998 (“DPA”).....	38
(f) The Official Secrets Act 1989 (“OSA”).....	38
(g) The Human Rights Act 1998 (“HRA”).....	39
3. The Interception of Communications Code of Practice	39
C. Acquisition of communications data.....	40
1. Chapter II of RIPA.....	40
2. The Acquisition and Disclosure of Communications Data: Code of Practice.....	41
3. News Group and Others v. The Commissioner of Police of the Metropolis IPT/14/176/H, 17 December 2015	69
4. The Police and Criminal Evidence Act 1984	71
D. IPT practice and procedure	71
1. RIPA	71
2. The Investigatory Powers Tribunal Rules 2000 (“the Rules”).....	72
3. IPT ruling on preliminary issues of law	73
4. Counsel to the Tribunal	75
E. Oversight.....	75
F. Reviews of interception operations by the intelligence service	76
1. Intelligence and Security Committee of Parliament: July 2013 Statement on GCHQ’s alleged interception of communications under the US PRISM programme.....	76
2. Privacy and security: a modern and transparent legal framework.....	77
3. “A Question of Trust”: Report of the Investigatory Powers Review by the Independent Reviewer of Terrorism Legislation (“the Anderson Report”).....	79
4. A Democratic Licence to Operate: Report of the Independent Surveillance Review (“ISR”).....	81
5. Report of the Bulk Powers Review	82
6. Attacks in London and Manchester March-June 2017: Independent Assessment of MI5 and Police Internal Reviews	83
7. Annual Report of the Interception of Communications Commissioner for 2016.....	85
(a) Section 8(4) warrants.....	85
(b) Acquisition of communications data under Chapter II of RIPA	88
G. The Investigatory Powers Act 2016.....	89
H. Relevant international law	91
1. The United Nations.....	91
(a) Resolution no. 68/167 on The Right to Privacy in the Digital Age	91
(b) The Constitution of the International Telecommunication Union 1992.....	91
(c) The 2006 Annual Report of the International Law Commission	91

BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

2. The Council of Europe.....	93
(a) The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981	93
(b) The Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows of 8 November 2001 (CETS No. 181)	95
(c) Recommendation of the Committee of Ministers on the protection of personal data in the area of telecommunication services.....	96
(d) The 2001 (Budapest) Convention on Cybercrime.....	96
(e) The 2015 Report of the European Commission for Democracy through Law (“the Venice Commission”) on the Democratic Oversight of Signals Intelligence Agencies	99
I. European Union law	100
1. Charter of Fundamental Rights of the European Union	100
Article 7 – Respect for private and family life	100
Article 8 – Protection of personal data	100
Article 11 – Freedom of expression and information	100
2. EU directives and regulations relating to protection and processing of personal data	100
3. Relevant case-law of the Court of Justice of the European Union (“CJEU”).....	103
(a) <i>Digital Rights Ireland v. Minister for Communications, Marine and Natural Resources and Others and Seitinger and Others</i> (Cases C-293/12 and C-594/12; ECLI:EU:C:2014:238)	103
(b) <i>Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others</i> (Cases C-203/15 and C-698/15; ECLI:EU:C:2016:970).....	105
(c) <i>Privacy International v. Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service and Secret Intelligence Service</i> (IPT/15/110/CH; EU OJ C 22, 22.1.2018, p. 29–30).....	106

BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

THE LAW.....107

I. EXHAUSTION OF DOMESTIC REMEDIES107

 A. The parties’ submissions.....107

 1. The Government.....107

 2. The applicants.....108

 B. The submissions of the third party.....109

 C. The Court’s assessment.....109

 1. General principles.....109

 2. Application of those principles to the case at hand111

II. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION117

 A. The section 8(4) regime118

 1. Admissibility.....118

 2. Merits.....118

 (a) The parties’ submissions118

 (i) The applicants118

 (ii) The Government.....120

 (b) The submissions of the third parties.....124

 (i) Article 19.....124

 (ii) Access Now.....124

 (iii) ENNHRI.....124

 (iv) The Helsinki Foundation for Human Rights (“HFHR”).....125

 (v) The International Commission of Jurists (“ICJ”).....125

 (vi) Open Society Justice Initiative (“OSJI”).....125

 (vii) European Digital Rights (“EDRi”) and other organisations
 active in the field of human rights in the information society125

 (viii) The Law Society of England and Wales.....126

 (c) The Court’s assessment.....126

 (i) General principles relating to secret measures of surveillance,
 including the interception of communications126

 (ii) Existing case-law on the bulk interception of communications.....129

 (iii) The test to be applied in the present case.....130

 B. The intelligence sharing regime150

 1. Admissibility.....150

 (a) The parties’ submissions150

 (b) The Court’s assessment.....151

 2. Merits.....153

 (a) The parties’ submissions153

 (i) The applicants153

 (ii) The Government.....153

 (b) The submissions of the third parties.....155

BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

(i) The Electronic Privacy Information Center (“EPIC”)	155
(ii) Access Now	155
(iii) Bureau Brandeis	155
(iv) Center for Democracy and Technology (“CDT”) and Pen American Center (“PEN America”)	156
(v) The International Commission of Jurists (“ICJ”)	156
(vi) Open Society Justice Initiative (“OSJI”)	156
(vii) The Law Society of England and Wales	156
(viii) Human Rights Watch (“HRW”)	157
(c) The Court’s assessment	157
(i) The scope of the applicants’ complaints	157
(ii) The nature of the interference	158
(iii) The applicable test	158
(iv) Application of the test to material falling into the second category	160
(v) Application of the test to material falling into the third category	165
C. The Chapter II regime	166
1. Admissibility	166
2. Merits	167
(a) The parties’ submissions	167
(i) The applicants	167
(ii) The Government	168
(b) The Court’s assessment	168
(i) Existing case-law on the acquisition of communications data	168
(ii) The approach to be taken in the present case	169
(iii) Examination of the Chapter II regime	170
III. ALLEGED VIOLATION OF ARTICLE 10 OF THE CONVENTION	170
A. Admissibility	171
1. The applicants in the third of the joined cases	171
2. The applicants in the second of the joined cases	172
B. Merits	172
1. The parties’ submissions	172
(a) The applicants	172
(b) The Government	173
2. The submissions of the third parties	174
(a) The Helsinki Foundation for Human Rights	174
(b) The National Union of Journalists (“NUJ”) and the International Federation of Journalists (“IFJ”)	174
(c) The Media Lawyers’ Association (“MLA”)	175

BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

3. The Court’s assessment	175
(a) General principles.....	175
(b) The application of the general principles to the present case.....	176
(i) The section 8(4) regime.....	176
(ii) The Chapter II regime	178
(iii) Overall conclusion	179
IV. ALLEGED VIOLATION OF ARTICLE 6 OF THE CONVENTION.....	179
V. ALLEGED VIOLATION OF ARTICLE 14 OF THE CONVENTION COMBINED WITH ARTICLES 8 AND 10 OF THE CONVENTION	181
VI. APPLICATION OF ARTICLE 41 OF THE CONVENTION.....	183
A. Damage	183
B. Costs and expenses.....	183
C. Default interest.....	183
FOR THESE REASONS, THE COURT:.....	184
APPENDIX.....	186
PARTLY CONCURRING, PARTLY DISSENTING OPINION OF JUDGE KOSKELO, JOINED BY JUDGE TURKOVIĆ.....	187
I. The RIPA section 8(4) regime.....	187
(i) The context of earlier case-law	187
(ii) The context of the present case	189
(iii) Concerns.....	190
II. The intelligence-sharing regime.....	194
JOINT PARTLY DISSENTING AND PARTLY CONCURRING OPINION OF JUDGES PARDALOS AND EICKE	195
<i>Introduction</i>	195
<i>Admissibility</i>	196
<i>The section 8(4) regime</i>	199
<i>Post Scriptum</i>	203

BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT 1

In the case of Big Brother Watch and Others v. the United Kingdom,
The European Court of Human Rights (First Section), sitting as a
Chamber composed of:

Linos-Alexandre Sicilianos, *President*,

Kristina Pardalos,

Aleš Pejchal,

Ksenija Turković,

Armen Harutyunyan,

Pauliine Koskelo,

Tim Eicke, *judges*,

and Abel Campos, *Section Registrar*,

Having deliberated in private on 7 November 2017 and 3 July 2018,

Delivers the following judgment, which was adopted on the
last-mentioned date:

PROCEDURE

1. The case originated in three applications (nos. 58170/13, 62322/14 and 24960/15) against the United Kingdom of Great Britain and Northern Ireland lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms (“the Convention”) by the companies, charities, organisations and individuals listed in the Appendix (“the applicants”) on 4 September 2013, 11 September 2014 and 20 May 2015 respectively.

2. The applicants were represented by Mr D. Carey, of Deighton Pierce Glynn Solicitors; Ms R. Curling of Leigh Day and Co. Solicitors; and Ms E. Norton of Liberty. The Government of the United Kingdom (“the Government”) were represented by their Agent, Ms R. Sagoo of the Foreign and Commonwealth Office.

3. The applicants complained about the scope and magnitude of the electronic surveillance programmes operated by the Government of the United Kingdom.

4. The applications were communicated to the Government on 7 January 2014, 5 January 2015 and 24 November 2015. In the first case, leave to intervene was granted to Human Rights Watch, Access Now, Bureau Brandeis, Center For Democracy & Technology, European Network of National Human Rights Institutions and the Equality and Human Rights Commission, the Helsinki Foundation For Human Rights, the International Commission of Jurists, Open Society Justice Initiative, The Law Society of England and Wales and Project Moore; in the second case, to the Center For Democracy & Technology, the Helsinki Foundation For Human Rights, the International Commission of Jurists, the National Union of Journalists and

2 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

the Media Lawyers' Association; and in the third case, to Article 19, the Electronic Privacy Information Center and to the Equality and Human Rights Commission.

5. On 4 July 2017 the Chamber of the First Section decided to join the applications and hold an oral hearing. That hearing took place in public in the Human Rights Building, Strasbourg, on 7 November 2017.

There appeared before the Court:

(a) *for the Government*

Ms R. SAGOO,	<i>Agent,</i>
Mr J. EADIE QC,	
Mr J. MILFORD,	<i>Counsel,</i>
Ms N. SAMUEL	
Mr S. BOWDEN,	
Mr M. ANSTEE,	
Mr T. RUTHERFORD,	
Ms L. MORGAN,	
Mr B. NEWMAN,	<i>Advisers.</i>

(b) *for the applicants*

Ms D. ROSE QC,	
Ms H. MOUNTFIELD QC,	
Mr M. RYDER QC,	<i>Counsel,</i>
Mr R. MEHTA,	
Mr C. MCCARTHY,	
Mr D. CAREY,	
Mr N. WILLIAMS	<i>Advisers.</i>

6. The Court heard addresses by Mr Eadie, Ms Rose and Ms Mountfield, as well as their replies to questions put by the President and by Judges Koskelo, Harutyunyan, Eicke, Turković and Pardalos.

THE FACTS

I. THE CIRCUMSTANCES OF THE CASE

A. Background

7. The three applications were introduced following revelations by Edward Snowden relating to the electronic surveillance programmes

operated by the intelligence services of the United States of America and the United Kingdom.

8. The applicants, who are listed in the Appendix, all believed that due to the nature of their activities, their electronic communications were likely to have either been intercepted by the United Kingdom intelligence services; obtained by the United Kingdom intelligence services after being intercepted by foreign governments; and/or obtained by the United Kingdom authorities from Communications Service Providers (“CSPs”).

B. The secret surveillance schemes

9. Internet communications are primarily carried over international submarine fibre optic cables operated by CSPs. Each cable may carry several “bearers”, and there are approximately 100,000 of these bearers joining up the global Internet. A single communication over the Internet is divided into “packets” (units of data) which may be transmitted separately across multiple bearers. These packets will travel via a combination of the quickest and cheapest paths, which may also depend on the location of the servers. Consequently, some or all of the parts of any particular communication sent from one person to another, whether within the United Kingdom or across borders, may be routed through one or more other countries if that is the optimum path for the CSPs involved.

1. Government Communications Headquarters (“GCHQ”)

10. The Edward Snowden revelations indicated that GCHQ (being one of the United Kingdom intelligence services) was running an operation, codenamed “TEMPORA”, which allowed it to tap into and store huge volumes of data drawn from bearers.

11. According to the March 2015 Report of the Intelligence and Security Committee of Parliament (“the ISC report” – see paragraphs 151-159 below), GCHQ is operating two major processing systems for the bulk interception of communications. The United Kingdom authorities have neither confirmed nor denied the existence of an operation codenamed TEMPORA.

12. The first of the two processing systems referred to in the ISC report is targeted at a very small percentage of bearers. As communications flow across the targeted bearers, the system compares the traffic against a list of “simple selectors”. These are specific identifiers (for example, an email address) relating to a known target. Any communications which match are collected; those that do not are automatically discarded. Analysts then carry out a “triage process” in relation to collected communications to determine which are of the highest intelligence value and should therefore be opened and read. In practice, only a very small proportion of the items collected

4 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

under this process are opened and read by analysts. GCHQ does not have the capacity to read all communications.

13. The second processing system is targeted at an even smaller number of bearers (a subset of those accessed by the process described in the paragraph above) which are deliberately targeted as those most likely to carry communications of intelligence interest. This second system has two stages: first, the initial application of a set of “processing rules” designed to discard material least likely to be of value; and secondly, the application of complex queries to the selected material in order to draw out those likely to be of the highest intelligence value. Those searches generate an index, and only items on that index may potentially be examined by analysts. All communications which are not on the list must be discarded.

14. The legal framework for bulk interception in force at the relevant time is set out in detail in the “Relevant Domestic law and practice” section below. In brief, section 8(4) of the Regulation of Investigatory Powers Act 2000 (“RIPA” – see paragraph 67 below) allows the Secretary of State to issue warrants for the “interception of external communications”, and pursuant to section 16 of RIPA (see paragraphs 78-85 below) intercepted material cannot 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”.

2. *The United States’ National Security Agency (“NSA”)*

15. The NSA has acknowledged the existence of two operations called PRISM and Upstream.

(a) PRISM

16. PRISM is a programme through which the United States’ Government obtains intelligence material (such as communications) from Internet Service Providers (“ISPs”). Access under PRISM is specific and targeted (as opposed to a broad “data mining” capability). The United States’ administration has stated that the programme is regulated under the Foreign Intelligence Service Act (“FISA”), and applications for access to material through PRISM have to be approved by the FISA Court, which is comprised of eleven senior judges.

17. Documents from the NSA leaked by Edward Snowden suggest that GCHQ has had access to PRISM since July 2010 and has used it to generate intelligence reports. GCHQ has acknowledged that it acquired information from the United States’ which had been obtained via PRISM.

(b) Upstream

18. According to the leaked documents, the Upstream programme allows the collection of content and communications data from fibre-optic

cables and infrastructure owned by United States' CSPs. This programme has broad access to global data, in particular that of non-US citizens, which can then be collected, stored and searched using keywords.

C. Domestic proceedings in the first and second of the joined cases

19. The applicants in the first of the joined cases (application no. 58170/13) sent a pre-action protocol letter to the Government on 3 July 2013 setting out their complaints and seeking declarations that sections 1 and 3 of the Intelligence Services Act (see paragraphs 100-103 below), section 1 of the Security Services Act (see paragraph 99 below) and section 8 of RIPA (see paragraph 67 below) were incompatible with the Convention. In their reply of 26 July 2013, the Government stated that the effect of section 65(2) of RIPA was to exclude the jurisdiction of the High Court in respect of human rights complaints against the intelligence services. These complaints could however be raised in the Investigatory Powers Tribunal ("IPT"), a court established under RIPA to hear allegations by citizens of wrongful interference with their communications as a result of conduct covered by that Act, which was endowed with exclusive jurisdiction to investigate any complaint that a person's communications have been intercepted and, where interception has occurred, to examine the authority for such interception (see paragraphs 123-143 below). No further action was taken by these applicants.

20. The applicants in the second of the joined cases (application no. 62322/14) did not bring any domestic proceedings as they did not believe that they had an effective remedy for their Convention complaints.

D. Domestic proceedings in the third of the joined cases

21. The ten human rights organisations which are the applicants in the third of the joined cases (application no. 24960/15) each lodged a complaint before the IPT between June and December 2013. They alleged that the intelligence services, the Home Secretary and the Foreign Secretary had acted in violation of Articles 8, 10, and 14 of the Convention by: (i) accessing or otherwise receiving intercepted communications and communications data from the US Government under the PRISM and Upstream programmes ("the PRISM issue"); and (ii) intercepting, inspecting and retaining their communications and their communications data under the TEMPORA programme ("the section 8(4) issue"). The applicants sought disclosure of all relevant material relied on by the intelligence services in the context of their interception activities and, in particular, all policies and guidance.

22. On 14 February 2014 the IPT ordered that the ten cases be joined. It subsequently appointed Counsel to the Tribunal (see paragraph 142 below),

whose function is to assist the IPT in whatever way it directs, including by making representations on issues in relation to which not all parties can be represented (for example, for reasons of national security).

23. In their response to the applicants' claims, the Government adopted a "neither confirm nor deny" approach, that is to say, they declined to confirm or deny whether the applicants' communications had actually been intercepted. It was therefore agreed that the IPT would determine the legal issues on the basis of assumed facts to the effect that the NSA had obtained the applicants' communications and communications data via PRISM or Upstream and had passed them to GCHQ, where they had been retained, stored, analysed and shared; and that the applicants' communications and communications data had been intercepted by GCHQ under the TEMPORA programme and had been retained, stored, analysed and shared. The question was whether, on these assumed facts, the interception, retention, storage and sharing of data was compatible with Articles 8 and 10, taken alone and together with Article 14 of the Convention.

1. The hearing

24. The IPT, composed of two High Court Judges (including the President), a Circuit Judge and two senior barristers, held a five-day, public hearing from 14-18 July 2014. The Government requested an additional closed hearing in order to enable the IPT to consider GCHQ's unpublished – described during the public hearing as "below the waterline" – internal arrangements for processing data. The applicants objected, arguing that the holding of a closed hearing was not justified and that the failure to disclose the arrangements to them was unfair.

25. The request for a closed hearing was granted pursuant to Rule 9 of the IPT's Rules of Procedure (see paragraph 131 below) and on 10 September 2014 a closed hearing took place, at which neither the applicants nor their representatives were present. Instead, the IPT was "assisted by the full, perceptive and neutral participation ... of Counsel to the Tribunal", who performed the following roles: (i) identifying documents, parts of documents or gists that ought properly to be disclosed; (ii) making such submissions in favour of disclosure as were in the interests of the Claimants and open justice; and (iii) ensuring that all the relevant arguments (from the Claimants' perspective) on the facts and the law were put before the IPT.

26. In the closed hearing, the IPT examined the internal arrangements regulating the conduct and practice of the intelligence services. It found that it was entitled to look "below the waterline" to consider the adequacy of the applicable safeguards and whether any further information could or should be disclosed to the public in order to comply with the requirements of Articles 8 and 10.

27. On 9 October 2014 the IPT notified the applicants that it was of the view that there was some closed material which could be disclosed. It explained that it had invited the Government to disclose the material and that the Government had agreed to do so. The material was accordingly provided to the applicants in a note (“the 9 October disclosure”) and the parties were invited to make submissions to the IPT on the disclosed material.

28. The applicants sought information on the context and source of the disclosure but the IPT declined to provide further details. The applicants made written submissions on the disclosure.

29. The respondents subsequently amended and amplified the disclosed material.

30. Following final disclosures made on 12 November 2014, the 9 October disclosure provided as follows:

“The US Government has publicly acknowledged that the Prism system and Upstream programme ... permit the acquisition of communications to, from, or about specific tasked selectors associated with non-US persons who are reasonably believed to be located outside the United States in order to acquire foreign intelligence information. To the extent that the Intelligence Services are permitted by the US Government to make requests for material obtained under the Prism system (and/or ... pursuant to the Upstream programme), those requests may only be made for unanalysed intercepted communications (and associated communications data) acquired in this way.

1. 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. a relevant interception warrant under [RIPA] has already been issued by the Secretary of State, the assistance of the foreign government 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
- b. 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 contravene the principle established in *Padfield v. Minister of Agriculture, Fisheries and Food* [1968] AC 997 [that a public body is required to exercise its discretionary powers to promote (and not to circumvent) the policy and the objects of the legislation which created those powers] (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. In these circumstances, the question whether the request should be made would be considered and decided upon by the Secretary of State personally. Any such request would only be made in exceptional circumstances, and has not occurred as at the date of this statement.

...

2. Where the Intelligence Services receive intercepted communications content or communications data from the government of a country or territory outside the United

8 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

Kingdom, irrespective of whether it is/they are solicited or unsolicited, whether the content is analysed or unanalysed, or whether or not the communications data are associated with the content of communications, the communications content and data are, pursuant to internal ‘arrangements’, subject to the same internal rules and safeguards as the same categories of content or data, when they are obtained directly by the Intelligence Services as a result of interception under RIPA.

3. Those of the Intelligence Services that receive unanalysed intercepted material and related communications data from interception under a s.8(4) warrant have internal ‘arrangements’ that require a record to be created, explaining why access to the unanalysed intercepted material is required, before an authorised person is able to access such material pursuant to s.16 of RIPA.

4. The internal ‘arrangements’ of those of the Intelligence Services that receive unanalysed intercepted material and related communications data from interception under a s.8(4) warrant specify (or require to be determined, on a system-by-system basis) maximum retention periods for different categories of such data which reflect the nature and intrusiveness of the particular data at issue. The periods so specified (or determined) are normally no longer than 2 years, and in certain cases are significantly shorter (intelligence reports that draw on such data are treated as a separate category, and are retained for longer). Data may only be retained for longer than the applicable maximum retention period where prior authorisation has been obtained from a senior official within the particular Intelligence Service at issue on the basis that continued retention of the particular data at issue has been assessed to be necessary and proportionate (if the continued retention of any such data is thereafter assessed no longer to meet the tests of necessity and proportionality, such data are deleted). As far as possible, all retention periods are implemented by a process of automated deletion which is triggered once the applicable maximum retention period has been reached for the data at issue. The maximum retention periods are overseen by, and agreed with the Commissioner. As regards related communications data in particular, Sir Anthony May made a recommendation to those of the Intelligence Services that receive unanalysed intercepted material and related communications data from interception under a s.8(4) warrant, and the interim Commissioner (Sir Paul Kennedy) has recently expressed himself to be content with the implementation of that recommendation.

5. The Intelligence Services’ internal ‘arrangements’ under [the Security Services Act 1989], [the Intelligence Services Act 1994] and ss.15-16 of RIPA are periodically reviewed to ensure that they remain up-to-date and effective. Further, the Intelligence Services are henceforth content to consider, during the course of such periodic reviews, whether more of those internal arrangements might safely and usefully be put into the public domain (for example, by way of inclusion in a relevant statutory Code of Practice).”

2. The IPT’s first judgment of 5 December 2014

31. The IPT issued its first judgment on 5 December 2014. The judgment addressed the arrangements then in place for intercepting and sharing data, making extensive reference throughout to this Court’s case-law.

(a) The PRISM issue

32. The IPT accepted that the PRISM issue engaged Article 8 of the Convention, albeit at a “lower level” than the regime under consideration in

Weber and Saravia v. Germany (dec.), no. 54934/00, ECHR 2006-XI. As a consequence, there would need to be compliance by the authorities involved in processing the data with the requirements of Article 8, particularly in relation to storage, sharing, retention and destruction. In the IPT's view, in order for the interference to be considered "in accordance with the law", there could not be unfettered discretion for executive action; rather, the nature of the rules had to be clear and the ambit of the rules had – in so far as possible – to be in the public domain (citing *Bykov v. Russia* [GC], no. 4378/02, §§ 76 and 78, 10 March 2009 and *Malone v. the United Kingdom*, 2 August 1984, Series A no. 82). However, it considered it plain that in the field of national security, much less was required to be put in the public domain and the degree of foreseeability required by Article 8 had to be reduced, otherwise the whole purpose of the steps taken to protect national security would be at risk (citing *Leander v. Sweden*, 26 March 1987, § 51, Series A no. 116).

33. The IPT continued:

"41. We consider that what is required is a sufficient signposting of the rules or arrangements insofar as they are not disclosed ... We are satisfied that in the field of intelligence sharing it is not to be expected that rules need to be contained in statute (*Weber*) or even in a code (as was required by virtue of the Court's conclusion in *Liberty v. [the United Kingdom]*, no. 58243/00, 1 July 2008]). It is in our judgment sufficient that:

- i) Appropriate rules or arrangements exist and are publicly known and confirmed to exist, with their content sufficiently signposted, such as to give an adequate indication of it (as per *Malone* ...).
- ii) They are subject to proper oversight."

34. The IPT noted that arrangements for information sharing were provided for in the statutory framework set out in the Security Services Act 1994 ("the SSA" – see paragraphs 98-99 below) and the Intelligence Services Act 1994 ("the ISA" – see paragraphs 100-103 below). It further referred to a witness statement of Charles Farr, the Director-General of the Office for Security and Counter Terrorism ("OSCT") at the Home Office, in which he explained that the statutory framework set out in those Acts was underpinned by detailed internal guidance, including arrangements for securing that the services only obtained the information necessary for the proper discharge of their functions. He further indicated that staff received mandatory training on the legal and policy framework in which they operated, including clear instructions on the need for strict adherence to the law and internal guidance. Finally, he stated that the full details of the arrangements were confidential since they could not be published safely without undermining the interests of national security.

35. The IPT therefore acknowledged that as the arrangements were not made known to the public, even in summary form, they were not accessible. However, the IPT considered it significant that the arrangements were

subject to oversight and investigation by the Intelligence and Security Committee of Parliament and the independent Interception of Communications Commissioner. Furthermore, it itself was in a position to provide oversight, having access to all secret information, and being able to adjourn into closed hearing to assess whether the arrangements referred to by Mr Farr existed and were capable of giving the individual protection against arbitrary interference.

36. In so far as the claimants challenged the IPT's decision to look "below the waterline" when assessing the adequacy of the safeguards, the IPT considered itself entitled to look at the internal arrangements in order to be satisfied that there were adequate safeguards and that what was described as "above the waterline" was accurate and gave a sufficiently clear signposting as to what was "below the waterline" without disclosing the detail of it. In this regard, the IPT did not accept that the holding of a closed hearing, as had been carried out in the applicants' case, was unfair. It accorded with the statutory procedure, gave the fullest and most transparent opportunity for hearing full arguments *inter partes* on hypothetical and actual facts with as much as possible heard in public, and protected the public interest and national security.

37. Having considered the arrangements "below the waterline", the IPT was satisfied that the 9 October disclosure (as subsequently amended) provided a clear and accurate summary of that part of the evidence given in the closed hearing which could and should be disclosed and that the rest of the evidence given in closed hearing was too sensitive for disclosure without risk to national security or to the "neither confirm nor deny" principle. It was further satisfied that it was clear that the preconditions for requesting information from the United States Government were either the existence of a section 8(1) warrant, or the existence of a section 8(4) warrant within whose ambit the proposed target's communications fell, together, if the individual was known to be in the British Islands, with a section 16(3) modification (see paragraph 80 below). In other words, any request pursuant to PRISM or Upstream in respect of intercept or communications data would be subject to the RIPA regime, unless it fell within the wholly exceptional scenario outlined in 1(b) of the material disclosed after the first hearing. However, a 1(b) request had never occurred.

38. The IPT nevertheless identified the following "matter of concern":

"Although it is the case that any request for, or receipt of, intercept or communications data pursuant to Prism and/or Upstream is ordinarily subject to the same safeguards as in a case where intercept or communication data are obtained directly by the Respondents, if there were a 1(b) request, albeit that such request must go to the Secretary of State, and that any material so obtained must be dealt with pursuant to RIPA, there is the possibility that the s.16 protection might not apply. As already indicated, no 1(b) request has in fact ever occurred, and there has thus been no problem hitherto. We are however satisfied that there ought to be introduced a

procedure whereby any such request, if it be made, when referred to the Secretary of State, must address the issue of s.16(3).”

39. However, subject to this caveat, the IPT reached the following conclusions:

“(i) Having considered the arrangements below the waterline, as described in this 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.

(ii) This is of course of itself not sufficient, because the arrangements must be sufficiently accessible to the public. We are satisfied that they are sufficiently signposted by virtue of the statutory framework to which we have referred and the Statements of the ISC and the Commissioner quoted above, and as now, after the two closed hearings that we have held, publicly disclosed by the Respondents and recorded in this judgment.

(iii) These arrangements are subject to oversight.

(iv) The scope of the discretion conferred on the Respondents to receive and handle intercepted material and communications data and (subject to the s.8(4) issues referred to below) the manner of its exercise, are accordingly (and consistent with *Bykov* - see paragraph 37 above) accessible with sufficient clarity to give the individual adequate protection against arbitrary interference.”

40. Finally, the IPT addressed an argument raised by Amnesty International only; namely, that the United Kingdom owed a positive obligation under Article 8 of the Convention to prevent or forestall the United States from intercepting communications including an obligation not to acquiesce in such interception by receiving its product. However, the IPT, citing *M. and Others v. Italy and Bulgaria*, no. 40020/03, § 127, 31 July 2012, noted that “the Convention organs have repeatedly stated that the Convention does not contain a right which requires a High Contracting Party to exercise diplomatic protection, or espouse an applicant’s complaints under international law, or otherwise to intervene with the authorities of another state on his or her behalf”. The IPT therefore rejected this submission.

(b) The section 8(4) issue

41. The IPT formulated four questions to be decided in order to determine whether the section 8(4) regime (which provided the legal framework for the bulk interception of external communications – see paragraph 67 below) was compatible with the Convention:

“(1) Is the difficulty of determining the difference between external and internal communications ... such as to cause the s.8(4) regime not to be in accordance with law contrary to Article 8(2)?

(2) Insofar as s.16 of RIPA is required as a safeguard in order to render the interference with Article 8 in accordance with law, is it a sufficient one?

12 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

(3) Is the regime, whether with or without s.16, sufficiently compliant with the *Weber* requirements, insofar as such is necessary in order to be in accordance with law?

(4) Is s. 16(2) indirectly discriminatory contrary to Article 14 of the Convention, and, if so, can it be justified?”

42. In relation to the first question, the applicants had contended that following the “sea-change in technology since 2000” substantially more communications were now external, and as a result the internal/external distinction in section 8(4) was no longer “fit for purpose”. While the IPT accepted that the changes in technology had been substantial, and that it was impossible to differentiate at interception stage between external and internal communications, it found that the differences in view as to the precise definition of “external communications” did not *per se* render the section 8(4) regime incompatible with Article 8 § 2. In this regard, it considered that the difficulty in distinguishing between “internal” and “external” communications had existed since the enactment of RIPA and the changes in technology had not materially added to the quantity or proportion of communications which could or could not be differentiated as being external or internal at the time of interception. At worst, they had “accelerated the process of more things in the world on a true analysis being external than internal”. In any case the distinction was only relevant at interception stage. The “heavy lifting” was done by section 16 of RIPA, which prevented intercepted material being 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” (see paragraphs 78-80 below). Furthermore, all communications intercepted under a section 8(4) warrant could only be considered for examination by reference to that section.

43. In respect of the second question, the IPT held that the section 16 safeguards, which applied only to intercept material and not to related communications data, were sufficient. Although it concluded that the *Weber* criteria also extended to communications data, it considered that there was adequate protection or safeguards by reference to section 15 (see paragraphs 72-77 below). In addition, insofar as section 16 offered greater protection for communications content than for communications data, the difference was justified and proportionate because communications data was necessary to identify individuals whose intercepted material was protected by section 16 (that is, individuals known to be in the British Islands).

44. Turning to the third question, the IPT concluded that the section 8(4) regime was sufficiently compliant with the *Weber* criteria and was in any event “in accordance with the law”. With regard to the first and second requirements, it considered that the reference to “national security” was sufficiently clear (citing *Esbester v. the United Kingdom* (dec.),

no. 18601/91, 2 April 1993 and *Kennedy v. the United Kingdom*, no. 26839/05, 18 May 2010); the absence of targeting at the interception stage was acceptable and inevitable, as it had been in *Weber*; on their face, the provisions of paragraph 5.2 of the Interception of Communications Code of Practice, together with paragraphs 2.4, 2.5, 5.3, 5.4, 5.5 and 5.6 were satisfactory; there was no call for search words to be included in an application for a warrant or in the warrant itself, as this would unnecessarily undermine and limit the operation of the warrant and might in any event be entirely unrealistic; and there was no requirement for the warrant to be judicially authorised.

45. In considering the third, fourth, fifth and sixth of the *Weber* criteria, the IPT had regard to the safeguards in sections 15 and 16 of RIPA, the Interception of Communications Code of Practice, and the “below the waterline arrangements”. It did not consider it necessary that the precise details of all the safeguards should be published or contained in either statute or code of practice. Particularly in the field of national security, undisclosed administrative arrangements, which by definition could be changed by the Executive without reference to Parliament, could be taken into account, provided that what is disclosed indicated the scope of the discretion and the manner of its exercise. This was particularly so when, as was the case here, the Code of Practice itself referred to the arrangements, and there was a system of oversight (being the Commissioner, the IPT itself, and the ISC) which ensured that these arrangements were kept under review. The IPT was satisfied that, as a result of what it had heard at the closed hearing and the 9 October disclosure as amended, there was no large databank of communications data being built up and that there were adequate arrangements in respect of the duration of the retention of data and its destruction. As with the PRISM issue, the IPT considered that the section 8(4) arrangements were sufficiently signposted in statute, in the Code of Practice, in the Interception of Communications Commissioner’s reports and, now, in its own judgment.

46. As regards the fourth and final question, the IPT did not make any finding as to whether there was in fact indirect discrimination on grounds of national origin as a result of the different regimes applicable to individuals located in the British Islands and those located outside, since it considered that any indirect discrimination was sufficiently justified on the grounds that it was harder to investigate terrorist and criminal threats from abroad. Given that the purpose of accessing external communications was primarily to obtain information relating to those abroad, the consequence of eliminating the distinction would be the need to obtain a certificate under section 16(3) of RIPA (which exceptionally allowed access to material concerning persons within the British Islands intercepted under a section 8(4) warrant – see paragraph 80 below) in almost every case, which would radically undermine the efficacy of the section 8(4) regime.

47. Finally, in respect of Article 10, the applicants argued that its protection applied to investigatory NGOs as to journalists. Amnesty initially alleged before the IPT that there were likely to be no adequate arrangements for material protected by legal professional privilege, a complaint which was subsequently “hived off” to be dealt with in the *Belhadj* case (see paragraphs 92-94 below), to which Amnesty was joined as an additional claimant. No similar argument was made in respect of NGO confidence until 17 November 2014 (the first and second open hearings having taken place in July and October 2014). As the IPT considered that this argument could have been raised at any time, in its judgment it had been raised “far too late” to be incorporated into the ambit of the proceedings.

48. With regard to the remaining Article 10 complaints, the IPT noted that there was no separate argument over and above that arising in respect of Article 8. Although the IPT observed that there might be a special argument relating to the need for judicial pre-authorisation of a warrant (referring to *Sanoma Uitgevers B.V. v. the Netherlands* [GC], no. 38224/03, 14 September 2010), it emphasised that the applicants’ case did not concern targeted surveillance of journalists or non-governmental organisations. In any case, in the context of untargeted monitoring via a section 8(4) warrant, it was “clearly impossible” to anticipate a judicial pre-authorisation prior to the warrant limited to what might turn out to impact upon Article 10. Although the IPT accepted that an issue might arise in the event that, in the course of examination of the contents, some question of journalistic confidence arose, it observed that there were additional safeguards in the Code of Practice in relation to treatment of such material.

49. Following the publication of the judgment, the parties were invited to make submissions on whether, prior to the disclosures made to the IPT, the legal regime in place in respect of the PRISM issue complied with Articles 8 and 10 and on the proportionality and lawfulness of any alleged interception of their communications. The IPT did not see any need for further submissions on the proportionality of the section 8(4) regime as a whole.

3. *The IPT’s second judgment of 6 February 2015*

50. In its second judgment of 6 February 2015, the IPT considered whether, prior to its December 2014 judgment, the PRISM or Upstream arrangements breached Article 8 and/or 10 of the Convention.

51. It agreed that it was only by reference to the 9 October disclosure as amended that it was satisfied the current regime was “in accordance with the law”. The IPT was of the view that without the disclosures made, there would not have been adequate signposting, as was required under Articles 8 and 10. It therefore made a declaration that prior to the disclosures made:

“23. ... [T]he regime governing the soliciting, receiving, storing and transmitting by UK authorities of private communications of individuals located in the UK, which

have been obtained by US authorities pursuant to Prism and/or ... Upstream, contravened Articles 8 or 10 ECHR, but now complies.”

4. The IPT’s third judgment of 22 June 2015 as amended by its 1 July 2015 letter

52. The third judgment of the IPT, published on 22 June 2015, determined whether the applicants’ communications obtained under PRISM or Upstream had been solicited, received, stored or transmitted by the United Kingdom authorities in contravention of Articles 8 and/or 10 of the Convention; and whether the applicants’ communications had been intercepted, viewed, stored or transmitted by the United Kingdom authorities so as to amount to unlawful conduct or in contravention of Articles 8 and/or 10.

53. The IPT made no determination in favour of eight of the ten applicants. In line with its usual practice where it did not find in favour of the claimant, it did not confirm whether or not their communications had been intercepted. However, in relation to two applicants the IPT made determinations. The identity of one of the organisations was wrongly noted in the judgment and the error was corrected by the IPT’s letter of 1 July 2015.

54. In respect of Amnesty International, the IPT found that email communications had been lawfully and proportionately intercepted and accessed pursuant to section 8(4) of RIPA but that the time-limit for retention permitted under the internal policies of GCHQ had been overlooked and the material had therefore been retained for longer than permitted. However, the IPT was satisfied that the material had not been accessed after the expiry of the relevant retention time-limit and that the breach could be characterised as a technical one. It amounted nonetheless to a breach of Article 8 and GCHQ was ordered to destroy any of the communications which had been retained for longer than the relevant period and to deliver one hard copy of the documents within seven days to the Interception of Communications Commissioner to retain for five years in case they were needed for any further legal proceedings. GCHQ was also ordered to provide a closed report within fourteen days confirming the destruction of the documents. No award of compensation was made.

55. In respect of the Legal Resources Centre, the IPT found that communications from an email address associated with the applicant had been intercepted and selected for examination under a section 8(4) warrant. Although it was satisfied the interception was lawful and proportionate and that selection for examination was proportionate, the IPT found that the internal procedure for selection was, in error, not followed. There had therefore been a breach of the Legal Resources Centre’s Article 8 rights. However, the IPT was satisfied that no use was made of the material and that no record had been retained so the applicant had not suffered material

detriment, damage or prejudice. Its determination therefore constituted just satisfaction and no compensation was awarded.

II. RELEVANT DOMESTIC LAW AND PRACTICE

A. The interception of communications

1. Warrants: general

56. Section 1(1) of RIPA renders unlawful the interception of any communication in the course of its transmission by means of a public postal service or a public telecommunication system unless it takes place in accordance with a warrant under section 5 (“intercept warrant”).

57. Section 5(2) allows the Secretary of State to authorise an intercept warrant if he believes: that it is necessary for the reasons set out in section 5(3), namely that it is in the interests of national security, for the purpose of preventing or detecting serious crime, or for safeguarding the economic well-being of the United Kingdom; and that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct. In assessing necessity and proportionality, account should be taken of whether the information sought under the warrant could reasonably be obtained by other means.

58. Section 81(2)(b) of RIPA defines “serious crime” as crime which satisfies one of the following criteria:

“(a) that the offence or one of the offences that is or would be constituted by the conduct is an offence for which a person who has attained the age of twenty-one and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more;

(b) that the conduct involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose.”

59. Section 81(5) provides:

“For the purposes of this Act detecting crime shall be taken to include–

(a) establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed; and

(b) the apprehension of the person by whom any crime was committed;

and any reference in this Act to preventing or detecting serious crime shall be construed accordingly ...”

60. Section 6 provides that in respect of the intelligence services, only the Director General of MI5, the Chief of MI6 and the Director of GCHQ may apply for an intercept warrant.

61. There are two types of intercept warrant to which sections 5 and 6 apply: a targeted warrant as provided for by section 8(1); and an untargeted warrant as provided for by section 8(4).

62. By virtue of section 9 of RIPA, a warrant issued in the interests of national security or for safeguarding the economic well-being of the United Kingdom shall cease to have effect at the end of six months, and a warrant issued for the purpose of detecting serious crime shall cease to have effect after three months. At any time before the end of those periods, the Secretary of State may renew the warrant (for periods of six and three months respectively) if he believes that the warrant continues to be necessary on grounds falling within section 5(3). The Secretary of State shall cancel an interception warrant if he is satisfied that the warrant is no longer necessary on grounds falling within section 5(3).

63. Pursuant to section 5(6), the conduct authorised by an interception warrant shall be taken to include the interception of communications not identified by the warrant if necessary to do what is expressly authorised or required by the warrant; and the obtaining of related communications data.

64. Section 21(4) defines “communications data” as

“(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, of 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.”

65. The March 2015 Acquisition and Disclosure of Communications Data Code of Practice refers to these three categories as “traffic data”, “service use information”, and “subscriber information”. Section 21(6) of RIPA further defines “traffic data” as data which identifies the person, apparatus, location or address to or from which a communication is transmitted, and information about a computer file or program accessed or run in the course of sending or receiving a communication.

66. Section 20 defines “related communications data”, in relation to a communication intercepted in the course of its transmission by means of a postal service or telecommunication system, as communications data “obtained by, or in connection with, the interception”; and which “relates to the communication or to the sender or recipient, or intended recipient, of the communication”.

2. Warrants: section 8(4)

(a) Authorisation

67. “Bulk interception” of communications is carried out pursuant to a section 8(4) warrant. Section 8(4) and (5) of RIPA allows the Secretary of State to issue a warrant for “the interception of external communications in the course of their transmission by means of a telecommunication system”.

68. At the time of issuing a section 8(4) warrant, the Secretary of State must also issue a certificate setting out a description of the intercepted material which he considers it necessary to examine, and stating that he considers the examination of that material to be necessary for the reasons set out in section 5(3) (that is, that it is necessary in the interests of national security, for the purpose of preventing or detecting serious crime, or for safeguarding the economic well-being of the United Kingdom).

(b) “External” communications

69. Section 20 defines “external communication” as “a communication sent or received outside the British Islands”.

70. In the course of the *Liberty* proceedings, Charles Farr, the Director General of the OSCT, indicated that two people in the United Kingdom who email each other are engaging in “internal communication” even if the email service was housed on a server in the United States of America; however, that communication may be intercepted as a “by-catch” of a warrant targeting external communications. On the other hand, a person in the United Kingdom who communicates with a search engine overseas is engaging in an external communication, as is a person in the United Kingdom who posts a public message (such as a tweet or Facebook status update), unless all the recipients of that message are in the British Islands.

71. Giving evidence to the Intelligence and Security Committee of Parliament in October 2014, the Secretary of State for the Foreign and Commonwealth considered that:

“• In terms of an email, if one or both of the sender or recipient is overseas then this would be an external communication.

• In terms of browsing the Internet, if an individual reads the Washington Post’s website, then they have ‘communicated’ with a web server located overseas, and that is therefore an external communication.

• In terms of social media, if an individual posts something on Facebook, because the web server is based overseas, this would be treated as an external communication.

• In terms of cloud storage (for example, files uploaded to Dropbox), these would be treated as external communications, because they have been sent to a web server overseas.”

3. *Specific safeguards under RIPA*

(a) **Section 15**

72. Pursuant to Section 15(1), it is the duty of the Secretary of State to ensure, in relation to all interception warrants, that such arrangements are in force as he considers necessary for securing that the requirements of subsections (2) and (3) are satisfied in relation to the intercepted material and any related communications data; and, in the case of warrants in relation to which there are section 8(4) certificates, that the requirements of section 16 are also satisfied.

73. Section 15(2) provides:

“The requirements of this subsection are satisfied in relation to the intercepted material and any related communications data if each of the following—

- (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.”

74. Section 15(3) provides:

“The requirements of this subsection are satisfied in relation to the intercepted material and any related communications data if each copy made of any 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.”

75. Pursuant to section 15(4), something is necessary for the authorised purposes if, and only if, it continues to be, or is likely to become, necessary as mentioned in section 5(3) of the Act (that is, it is necessary in the interests of national security, for the purpose of preventing or detecting serious crime; for the purpose of safeguarding the economic well-being of the United Kingdom; or for the purpose of giving effect to the provisions of any international mutual assistance agreement); it is necessary for facilitating the carrying out of any of the interception functions of the Secretary of State; it is necessary for facilitating the carrying out of any functions of the Interception of Communications Commissioner or of the IPT; it is necessary to ensure 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; or it is necessary for the performance of any duty imposed on any person under public records legislation.

76. Section 15(5) requires the arrangements in place to secure compliance with section 15(2) to include such arrangements as the Secretary

20 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

of State considers necessary for securing that every copy of the material or data that is made is stored, for so long as it is retained, in a secure manner.

77. Pursuant to section 15(6), the arrangements to which section 15(1) refers are not required to secure that the requirements of section 15(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. However, such arrangements are required to secure, in the case of every such warrant, that possession of the intercepted material and data and of copies of the material or data is surrendered to authorities of a country or territory outside the United Kingdom only if the requirements of section 15(7) are satisfied. Section 15(7) provides:

“The requirements of this subsection are satisfied in the case of a warrant if it appears to the Secretary of State—

(a) that requirements corresponding to those of subsections (2) and (3) will apply, to such extent (if any) as the Secretary of State thinks fit, in relation to any of the intercepted material or related communications data possession of which, or of any copy of which, is surrendered to the authorities in question; and

(b) that restrictions are in force which would prevent, to such extent (if any) as the Secretary of State thinks fit, the doing of anything in, for the purposes of or in connection with any proceedings outside the United Kingdom which would result in such a disclosure as, by virtue of section 17, could not be made in the United Kingdom.”

(b) Section 16

78. Section 16 sets out additional safeguards in relation to the interception of “external” communications under section 8(4) warrants. Section 16(1) requires that intercepted material may only be read, looked at or listened to by the persons to whom it becomes available by virtue of the warrant if and to the extent that it has been certified as material the examination of which is necessary as mentioned in section 5(3) of the Act; and falls within section 16(2). Section 20 defines “intercepted material” as the contents of any communications intercepted by an interception to which the warrant relates.

79. Section 16(2) provides:

“Subject to subsections (3) and (4), 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.”

80. Pursuant to section 16(3), intercepted material falls within section 16(2), notwithstanding that it is selected by reference to one of the factors mentioned in that subsection, if 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) of the Act; and the material relates only to communications sent during a period specified in the certificate that is no longer than the permitted maximum.

81. The “permitted maximum” is defined in section 16(3A) as follows:

- “(a) in the case of material the examination of which is certified for the purposes of section 8(4) as necessary in the interests of national security, six months; and
- (b) in any other case, three months.”

82. Pursuant to section 16(4), intercepted material also falls within section 16(2), even if it is selected by reference to one of the factors mentioned in that subsection, if the person to whom the warrant is addressed believes, on reasonable grounds, that the circumstances are such that the material would fall within that subsection; or the conditions set out in section 16(5) are satisfied in relation to the selection of the material.

83. Section 16(5) provides:

- “Those conditions are satisfied in relation to the selection of intercepted material if –
- (a) it has appeared to the person to whom the warrant is addressed that there has been such a relevant change of circumstances as, but for subsection (4)(b), would prevent the intercepted material from falling within subsection (2);
- (b) since it first so appeared, a written authorisation to read, look at or listen to the material has been given by a senior official; and
- (c) the selection is made before the end of the permitted period.”

84. Pursuant to section 16(5A), the “permitted period” means:

- “(a) in the case of material the examination of which is certified for the purposes of section 8(4) as necessary in the interests of national security, the period ending with the end of the fifth working day after it first appeared as mentioned in subsection (5)(a) to the person to whom the warrant is addressed; and
- (b) in any other case, the period ending with the end of the first working day after it first so appeared to that person.”

85. Section 16(6) explains that a “relevant change of circumstances” means that it appears that either the individual in question has entered the British Islands; or that a belief by the person to whom the warrant is addressed in the individual’s presence outside the British Islands was in fact mistaken.

86. Giving evidence to the Intelligence and Security Committee of Parliament in October 2014, the Secretary of State for the Foreign and Commonwealth explained that:

22 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

“When an analyst selects communications that have been intercepted under the authority of an 8(4) warrant for examination, it does not matter what form of communication an individual uses, or whether his other communications are stored on a dedicated mail server or in cloud storage physically located in the UK, the US or anywhere else (and in practice the individual user of cloud services will not know where it is stored). If he or she is known to be in the British Islands it is not permissible to search for his or her communications by use of his or her name, e-mail address or any other personal identifier.”

4. *The Interception of Communications Code of Practice*

87. Section 71 of RIPA provides for the adoption of codes of practice by the Secretary of State in relation to the exercise and performance of his powers and duties under the Act. Draft codes of practice must be laid before Parliament and are public documents. They can only enter into force in accordance with an order of the Secretary of State. The Secretary of State can only make such an order if a draft of the order has been laid before Parliament and approved by a resolution of each House.

88. Under section 72(1) of RIPA, a person exercising or performing any power or duty relating to interception of communications must have regard to the relevant provisions of a code of practice. The provisions of a code of practice may, in appropriate circumstances, be taken into account by courts and tribunals under section 72(4) RIPA.

89. The Interception of Communication Code of Practice (“the IC Code”) was issued pursuant to section 71 of RIPA. The IC Code currently in force was issued in 2016.

90. Insofar as relevant, the IC Code provides:

“3.2. There are a limited number of persons who can make an application for an interception warrant, or an application can be made on their behalf. These are:

- The Director-General of the Security Service.
- The Chief of the Secret Intelligence Service.
- The Director of the Government Communications Headquarters (GCHQ).
- The Director-General of the National Crime Agency (NCA handles interception on behalf of law enforcement bodies in England and Wales).
- The Chief Constable of the Police Service of Scotland.
- The Commissioner of the Police of the Metropolis (the Metropolitan Police Counter Terrorism Command handles interception on behalf of Counter Terrorism Units, Special Branches and some police force specialist units in England and Wales).
- The Chief Constable of the Police Service of Northern Ireland.
- The Commissioners of Her Majesty’s Revenue & Customs (HMRC).
- The Chief of Defence Intelligence.

- A person who, for the purposes of any international mutual assistance agreement, is the competent authority of a country or territory outside the UK.

3.3. Any application made on behalf of one of the above must be made by a person holding office under the Crown.

3.4. All interception warrants are issued by the Secretary of State. Even where the urgency procedure is followed, the Secretary of State personally authorises the warrant, although it is signed by a senior official.

Necessity and proportionality

3.5. Obtaining a warrant under RIPA will only ensure that the interception authorised is a justifiable interference with an individual's rights under Article 8 (right to respect for private and family life) of the European Convention on Human Rights (ECHR) if it is necessary and proportionate for the interception to take place. RIPA recognises this by first requiring that the Secretary of State believes that the authorisation is necessary for one or more of the following statutory grounds:

- In the interests of national security;
- To prevent or detect serious crime;
- To safeguard the economic well-being of the UK so far as those interests are also relevant to the interests of national security.

3.6. These purposes are set out in section 5(3) of RIPA. The Secretary of State must also believe that the interception is proportionate to what is sought to be achieved by that conduct. Any assessment of proportionality involves balancing the seriousness of the intrusion into the privacy or property of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative, operational or capability terms. The warrant will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that there is a potential threat to national security (for example) may not alone render the most intrusive actions proportionate. No interference should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

3.7. The following elements of proportionality should therefore 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;
- 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;
- 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.

...

24 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

Duration of interception warrants

3.18. Interception warrants issued on serious crime grounds are valid for an initial period of three months. Interception warrants issued on national security/economic well-being of the UK grounds are valid for an initial period of six months. A warrant issued under the urgency procedure (on any grounds) is valid for five working days following the date of issue unless renewed by the Secretary of State.

3.19. Upon renewal, warrants issued on serious crime grounds are valid for a further period of three months. Warrants renewed on national security/economic well-being of the UK grounds are valid for a further period of six months. These dates run from the date on the renewal instrument.

3.20. Where modifications to an interception warrant are made, the warrant expiry date remains unchanged. However, where the modification takes place under the urgency provisions, the modification instrument expires after five working days following the date of issue, unless it is renewed in line with the routine procedure.

3.21. Where a change in circumstance leads the intercepting agency to consider it no longer necessary, proportionate or practicable for a warrant to be in force, the agency must make a recommendation to the Secretary of State that it should be cancelled with immediate effect.

...

4. SPECIAL RULES ON INTERCEPTION WITH A WARRANT

Collateral intrusion

4.1. Consideration should be given to any interference with the privacy of individuals who are not the subject of the intended interception, especially where communications relating to religious, medical, journalistic or legally privileged material may be involved, or where communications between a Member of Parliament and another person on constituency business may be involved or communications between a Member of Parliament and a whistle-blower. An application for an interception warrant should state whether the interception is likely to give rise to a degree of collateral infringement of privacy. A person applying for an interception warrant must also consider measures, including the use of automated systems, to reduce the extent of collateral intrusion. Where it is possible to do so, the application should specify those measures. These circumstances and measures will be taken into account by the Secretary of State when considering a warrant application made under section 8(1) of RIPA. Should an interception operation reach the point where individuals other than the subject of the authorisation are identified as investigative targets in their own right, consideration should be given to applying for separate warrants covering those individuals.

Confidential information

4.2. 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.

BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT 25

4.3. 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. See also paragraphs 4.26 and 4.28 – 4.31 for additional safeguards that should be applied in respect of confidential journalistic material.

...

Communications involving confidential journalistic material, confidential personal information and communications between a Member of Parliament and another person on constituency business

4.26. Particular consideration must also be given to the interception of communications that involve confidential journalistic material, confidential personal information, or communications between a Member of Parliament and another person on constituency business. Confidential journalistic material is explained at paragraph 4.3. Confidential personal information is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and the material in question relates to his or her physical or mental health or to spiritual counselling. Such information can include both oral and written communications. Such information as described above is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence, or is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. For example, confidential personal information might include consultations between a health professional and a patient, or information from a patient's medical records.

...

4.28. Where the intention is to acquire confidential personal information, the reasons should be clearly documented and the specific necessity and proportionality of doing so should be carefully considered. If the acquisition of confidential personal information is likely but not intended, any possible mitigation steps should be considered and, if none is available, consideration should be given to whether special handling arrangements are required within the intercepting agency.

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.

4.32. The safeguards set out in paragraphs 4.28 – 4.31 also apply to any section 8(4) material (see chapter 6) which is selected for examination and which constitutes confidential information.

...

6. INTERCEPTION WARRANTS (SECTION 8(4))

6.1. This section applies to the interception of external communications by means of a warrant complying with section 8(4) of RIPA.

6.2. In contrast to section 8(1), a section 8(4) warrant instrument need not name or describe the interception subject or a set of premises in relation to which the interception is to take place. Neither does section 8(4) impose an express limit on the number of external communications which may be intercepted. For example, if the requirements of sections 8(4) and (5) are met, then the interception of all communications transmitted on a particular route or cable, or carried by a particular CSP, could, in principle, be lawfully authorised. This reflects the fact that section 8(4) interception is an intelligence gathering capability, whereas section 8(1) interception is primarily an investigative tool that is used once a particular subject for interception has been identified.

6.3. Responsibility for the issuing of interception warrants under section 8(4) of RIPA rests with the Secretary of State. When the Secretary of State issues a warrant of this kind, it must be accompanied by a certificate. The certificate ensures that a selection process is applied to the intercepted material so that only material described in the certificate is made available for human examination. If the intercepted material cannot be selected to be read, looked at or listened to with due regard to proportionality and the terms of the certificate, then it cannot be read, looked at or listened to by anyone.

Section 8(4) interception in practice

6.4. 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.

Definition of external communications

6.5. 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 the 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 external communication for the purposes of section 20 of RIPA, whether or not it is routed via IP addresses outside the British Islands, because the sender and intended recipient are within the British Islands.

Intercepting non-external communications under section 8(4) warrants

6.6. Section 5(6)(a) of RIPA makes clear that the conduct authorised by a section 8(4) warrant may, in principle, include the interception of communications which are not external communications to the extent this is necessary in order to intercept the external communications to which the warrant relates.

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 communications 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.

Application for a section 8(4) warrant

6.8. An application for a warrant is made to the Secretary of State. Interception warrants, when issued, are addressed to the person who submitted the application. The purpose of such a warrant will typically reflect one or more of the intelligence priorities set by the National Security Council (NSC).

6.9. Prior to submission, each application is subject to a review within the agency making the application. This involves scrutiny by more than one official, who will consider whether the application is for a purpose falling within section 5(3) of RIPA and whether the interception proposed is both necessary and proportionate.

6.10. Each application, a copy of which must be retained by the applicant, should contain the following information:

- Background to the operation in question:
 - Description of the communications to be intercepted, details of the CSP(s) and an assessment of the feasibility of the operation where this is relevant; and
 - Description of the conduct to be authorised, which must be restricted to the interception of external communications, or the conduct (including the interception of other communications not specifically identified by the warrant as foreseen under section 5(6)(a) of RIPA) it is necessary to undertake in order to carry out what is authorised or required by the warrant, and the obtaining of related communications data.
- The certificate that will regulate examination of intercepted material;
- An explanation of why the interception is considered to be necessary for one or more of the section 5(3) purposes;
- A consideration of why the conduct to be authorised by the warrant is proportionate to what is sought to be achieved by that conduct;
- Where an application is urgent, supporting justification;

28 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

- 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 sections 16(2)-16(6) of RIPA; and
- An assurance that all material intercepted will be handled in accordance with the safeguards required by sections 15 and 16 of RIPA (see paragraphs 7.2 and 7.10 respectively).

Authorisation of a section 8(4) warrant

6.11. Before issuing a warrant under section 8(4), the Secretary of State must believe the warrant is necessary:

- In the 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 UK so far as those interests are also relevant to the interests of national security.

6.12. The power to issue an interception warrant for the purpose of safeguarding the economic well-being of the UK (as provided for by section 5(3)(c) of RIPA), may only be exercised where it appears to the Secretary of State that the circumstances are relevant to the interests of national security. The Secretary of State will not issue a warrant on section 5(3)(c) grounds if a direct link between the economic well-being of the UK and national security is not established. Any application for a warrant on section 5(3)(c) grounds should therefore identify the circumstances that are relevant to the interests of national security.

6.13. The Secretary of State must also consider that the conduct authorised by the warrant is proportionate to what it seeks to achieve (section 5(2)(b)). In considering necessity and proportionality, the Secretary of State must take into account whether the information sought could reasonably be obtained by other means (section 5(4)).

6.14. When the Secretary of State issues a warrant of this kind, it must be accompanied by a certificate in which the Secretary of State certifies that he or she considers examination of the intercepted material to be necessary for one or more of the section 5(3) purposes. 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.

6.15. The Secretary of State has a duty to ensure that arrangements are in force for securing that only that material which has been certified as necessary for examination for a section 5(3) purpose, and which meets the conditions set out in section 16(2) to section 16(6) is, in fact, read, looked at or listened to. The Interception of Communications Commissioner is under a duty to review the adequacy of those arrangements.

Urgent authorisation of a section 8(4) warrant

6.16. RIPA makes provision (section 7(1)(b)) for cases in which an interception warrant is required urgently, yet the Secretary of State is not available to sign the

warrant. In these cases the Secretary of State will still personally authorise the interception but the warrant is signed by a senior official, following discussion of the case between officials and the Secretary of State. RIPA restricts the issue of warrants in this way to urgent cases where the Secretary of State has personally and expressly authorised the issue of the warrant (section 7(2)(a)), and requires the warrant to contain a statement to that effect (section 7(4)(a)).

6.17. A warrant issued under the urgency procedure lasts for five working days following the date of issue unless renewed by the Secretary of State, in which case it expires after three months in the case of serious crime or six months in the case of national security or economic well-being, in the same way as other section 8(4) warrants.

Format of a section 8(4) warrant

6.18. Each warrant is addressed to the person who submitted the application. A copy may then be served upon such providers of communications services as he or she believes will be able to assist in implementing the interception. CSPs will not normally receive a copy of the certificate. The warrant should include the following:

- A description of the communications to be intercepted;
- The warrant reference number; and
- Details of the persons who may subsequently modify the certificate applicable to the warrant in an urgent case (if authorised in accordance with section 10(7) of RIPA).

Modification of a section 8(4) warrant and/or certificate

6.19. Interception warrants and certificates may be modified under the provisions of section 10 of RIPA. A warrant may only be modified by the Secretary of State or, in an urgent case, by a senior official with the express authorisation of the Secretary of State. In these cases a statement of that fact must be endorsed on the modifying instrument, and the modification ceases to have effect after five working days following the date of issue unless it is endorsed by the Secretary of State.

6.20. A certificate must be modified by the Secretary of State, except in an urgent case where a certificate may be modified by a senior official provided that the official holds a position in which he or she is expressly authorised by provisions contained in the certificate to modify the certificate on the Secretary of State's behalf, or the Secretary of State has expressly authorised the modification and a statement of that fact is endorsed on the modifying instrument. In the latter case, the modification ceases to have effect after five working days following the date of issue unless it is endorsed by the Secretary of State.

6.21. Where the Secretary of State is satisfied that it is necessary, a certificate may be modified to authorise the selection of communications of an individual in the British Islands. An individual's location should be assessed using all available information. If it is not possible, to determine definitively where the individual is located using that information, an informed assessment should be made, in good faith, as to the individual's location. If an individual is strongly suspected to be in the UK, the arrangements set out in this paragraph will apply.

Renewal of a section 8(4) warrant

6.22. The Secretary of State may renew a warrant at any point before its expiry date. Applications for renewals are made to the Secretary of State and contain an

update of the matters outlined in paragraph 6.10 above. In particular, 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 purposes in section 5(3), and why it is considered that interception continues to be proportionate.

6.23. Where the Secretary of State is satisfied that the interception continues to meet the requirements of RIPA, the Secretary of State may renew the warrant. Where the warrant is issued on serious crime grounds, the renewed warrant is valid for a further three months. Where it is issued on national security/economic well-being grounds the renewed warrant is valid for six months. These dates run from the date of signature on the renewal instrument.

6.24. In those circumstances where the assistance of CSPs has been sought, a copy of the warrant renewal instrument will be forwarded to all those on whom a copy of the original warrant instrument has been served, providing they are still actively assisting. A renewal instrument will include the reference number of the warrant or warrants being renewed under this single instrument.

Warrant cancellation

6.25. The Secretary of State must cancel an interception warrant if, at any time before its expiry date, he or she is satisfied that the warrant is no longer necessary on grounds falling within section 5(3) of RIPA. Intercepting agencies will therefore need to keep their warrants under continuous review and must notify the Secretary of State if they assess that the interception is no longer necessary. In practice, the responsibility to cancel a warrant will be exercised by a senior official in the warrant issuing department on behalf of the Secretary of State.

6.26. The cancellation instrument will be addressed to the person to whom the warrant was issued (the intercepting agency). A copy of the cancellation instrument should be sent to those CSPs, if any, who have given effect to the warrant during the preceding twelve months.

Records

6.27. The oversight regime allows the Interception of Communications Commissioner to inspect the warrant application upon which the Secretary of State's decision is based, and the interception agency may be required to justify the content. Each intercepting agency should keep the following to be made available for scrutiny by the Commissioner as he or she may require:

- All applications made for warrants complying with section 8(4), and applications made for the renewal of such warrants;
- All warrants and certificates, and copies of renewal and modification instruments (if any);
- Where any application is refused, the grounds for refusal as given by the Secretary of State;
- The dates on which interception started and stopped.

6.28. Records should also be kept of the arrangements for securing that only material which has been certified for examination for a purpose under section 5(3) and which meets the conditions set out in section 16(2) – 16(6) of RIPA in accordance with section 15 of RIPA is, in fact, read, looked at or listened to. Records should be kept of the arrangements by which the requirements of section 15(2) (minimisation of

copying and distribution of intercepted material) and section 15(3) (destruction of intercepted material) are to be met. For further details see the chapter on “Safeguards”.

7. SAFEGUARDS

7.1. All material intercepted under the authority of a warrant complying with section 8(1) or section 8(4) of RIPA and any related communications data must be handled in accordance with safeguards which the Secretary of State has approved in conformity with the duty imposed on him or her by RIPA. These safeguards are made available to the Interception of Communications Commissioner, and they must meet the requirements of section 15 of RIPA which are set out below. In addition, the safeguards in section 16 of RIPA apply to warrants complying with section 8(4). Any breach of these safeguards must be reported to the Interception of Communications Commissioner. The intercepting agencies must keep their internal safeguards under periodic review to ensure that they remain up-to-date and effective. During the course of such periodic reviews, the agencies must consider whether more of their internal arrangements might safely and usefully be put into the public domain.

The section 15 safeguards

7.2. Section 15 of RIPA requires that disclosure, copying and retention of intercepted material is limited to the minimum necessary for the authorised purposes. Section 15(4) of RIPA provides that something is necessary for the authorised purposes if the intercepted material:

- Continues to be, or is likely to become, necessary for any of the purposes set out in section 5(3) – namely, in the interests of national security, for the purpose of preventing or detecting serious crime, or for the purpose, in circumstances appearing to the Secretary of State to be relevant to the interests of national security, of safeguarding the economic well-being of the UK;
- Is necessary for facilitating the carrying out of the functions of the Secretary of State under Chapter I of Part I of RIPA;
- Is necessary for facilitating the carrying out of any functions of the Interception of Communications Commissioner or the Tribunal;
- Is necessary to ensure that a person conducting a criminal prosecution has the information needed to determine what is required of him or her by his or her duty to secure the fairness of the prosecution; or
- Is necessary for the performance of any duty imposed by the Public Record Acts.

Dissemination of intercepted material

7.3. The number of persons to whom any of the intercepted material is disclosed, and the extent of disclosure, is 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. It is enforced by prohibiting disclosure to persons who have not been appropriately vetted 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 or she needs to know about the intercepted material to carry out those duties. In the same way, only so much of the intercepted

material may be disclosed as the recipient needs. For example, if a summary of the intercepted 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 intercepted material is subsequently disclosed. In some cases this will be achieved by requiring the latter to obtain the originator's permission before disclosing the intercepted 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.

Copying

7.6. 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 intercepted material, but also extracts and summaries which identify themselves as the product of an interception, and any record referring to an interception which includes 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.

Storage

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 requirement to store intercept product securely applies to all those who are responsible for handling it, including CSPs. The details of what such a requirement will mean in practice for CSPs will be set out in the discussions they have with the Government before a Section 12 Notice is served (see paragraph 3.13).

Destruction

7.8. Intercepted material, and all copies, extracts and summaries which can be identified as the product of an interception, must be marked for deletion and securely destroyed as soon as possible once it is no longer needed for any of the authorised purposes. If such intercepted 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.

Personnel security

7.10. 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.

The section 16 safeguards

7.11. Section 16 provides for additional safeguards in relation to intercepted material gathered under section 8(4) warrants, requiring that the safeguards:

- Ensure that intercepted material is read, looked at or listened to by any person only to the extent that the intercepted material is certified; and
- Regulate the use of selection factors that refer to the communications of individuals known to be currently in the British Islands.

7.12. In addition, any individual selection of intercepted material must be proportionate in the particular circumstances (given section 6(1) of the Human Rights Act 1998).

7.13. The certificate ensures that a selection process is applied to material intercepted under section 8(4) warrants so that only material described in the certificate is made available for human examination (in the sense of being read, looked at or listened to). No official is permitted to gain access to the data other than as permitted by the certificate.

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

34 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

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 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.

7.20. The Secretary of State must ensure that the safeguards are in force before any interception under section 8(4) warrants can begin. The Interception of Communications Commissioner is under a duty to review the adequacy of the safeguards.

...

10. OVERSIGHT

10.1. RIPA provides for an Interception of Communications Commissioner, whose remit is to provide independent oversight of the use of the powers contained within the warranted interception regime under Chapter I of Part I of RIPA.

10.2. The Commissioner carries out biannual inspections of each of the nine interception agencies. The primary objectives of the inspections are to ensure that the Commissioner has the information he or she requires to carry out his or her functions under section 57 of RIPA and produce his or her report under section 58 of RIPA. This may include inspection or consideration of:

- The systems in place for the interception of communications;
- The relevant records kept by the intercepting agency;
- The lawfulness of the interception carried out; and
- Any errors and the systems designed to prevent such errors.

10.3. Any person who exercises the powers in RIPA Part I Chapter I must report to the Commissioner any action that is believed to be contrary to the provisions of RIPA or any inadequate discharge of section 15 safeguards. He or she must also comply with any request made by the Commissioner to provide any such information as the Commissioner requires for the purpose of enabling him or her to discharge his or her functions.”

5. *Statement of Charles Farr*

91. In his witness statement prepared for the *Liberty* proceedings, Charles Farr indicated that, beyond the details set out in RIPA, the 2010 Code, and the draft 2016 Code (which had at that stage been published for consultation), the full details of the sections 15 and 16 safeguards were kept confidential. He had personally reviewed the arrangements and was satisfied that they could not safely be put in the public domain without undermining the effectiveness of the interception methods. However, the arrangements were made available to the Commissioner who is required by RIPA to keep them under review. Furthermore, each intercepting agency was required to keep a record of the arrangements in question and any breach must be reported to the Commissioner.

6. *Belhadj and Others v. Security Service, Secret Intelligence Service, Government Communications Headquarters, the Secretary of State for the Home Department, and the Secretary of State for the Foreign and Commonwealth Office, IPT/13/132-9/H and IPT/14/86/CH*

92. The applicants in this case complained of breaches of Articles 6, 8 and 14 of the Convention arising from the alleged interception of their legally privileged communications. Insofar as Amnesty International, in the course of the *Liberty* proceedings, complained about the adequacy of the arrangements for the protection of material protected by legal professional privilege (“LPP”), those complaints were “hived off” to be dealt with in this case, and Amnesty International was joined as a claimant (see paragraph 47 above).

93. In the course of the proceedings, the respondents conceded that by virtue of there not being in place a lawful system for dealing with LPP, from January 2010 the regime for the interception/obtaining, analysis, use,

disclosure and destruction of legally privileged material had not been in accordance with the law for the purposes of Article 8 § 2 of the Convention and was accordingly unlawful. The Security Service and GCHQ confirmed that they would work in the forthcoming weeks to review their policies and procedures in light of the draft Interception Code of Practice and otherwise.

94. The IPT subsequently held a closed hearing, with the assistance of Counsel to the Tribunal (see paragraph 142 below), to consider whether any documents or information relating to any legally privileged material had been intercepted or obtained by the respondents. In a determination of 29 March 2015 it found that only two documents containing material subject to legal professional privilege of any of the claimants had been held by the agencies, and they neither disclosed nor referred to legal advice. It therefore found that the claimant concerned had not suffered any detriment or damage, and that the determination provided adequate just satisfaction. It nevertheless required that GCHQ provide an undertaking that those parts of the documents containing legally privileged material would be destroyed or deleted; that a copy of the documents would be delivered to the Interception of Communications Commissioner to be retained for five years; and that a closed report would be provided within fourteen days confirming the destruction and deletion of the documents.

95. Draft amendments to both the Interception of Communications Code of Practice and the Acquisition of Communications Data Code of Practice were subsequently put out for consultation and the Codes which were adopted as a result contained expanded sections concerning access to privileged information.

B. Intelligence sharing

1. British-US Communication Intelligence Agreement

96. A British-US Communication Intelligence Agreement of 5 March 1946 governs the arrangements between the British and United States authorities in relation to the exchange of intelligence information relating to “foreign” communications, defined by reference to countries other than the United States, the United Kingdom and the Commonwealth. Pursuant to the agreement, the parties undertook to exchange the products of a number of interception operations relating to foreign communications.

2. Relevant statutory framework for the operation of the intelligence services

97. There are three intelligence services in the United Kingdom: the security service (“MI5”), the secret intelligence service (“MI6”) and GCHQ.

(a) MI5

98. Pursuant to section 2 of the Security Services Act 1989 (“SSA”), it is the duty of the Director-General of MI5, who is appointed by the Secretary of State, to ensure that there are arrangements for securing that no information is obtained by MI5 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.

99. According to section 1 of the SSA, the functions of MI5 are 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; to safeguard the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands; and to act in support of the activities of police forces, the National Crime Agency and other law enforcement agencies in the prevention and detection of serious crime.

(b) MI6

100. Section 2 of the Intelligence Services Act 1994 (“ISA”) provides that the duties of the Chief of Service of MI6, who is appointed by the Secretary of State, include ensuring that there are arrangements for securing that no information is obtained by MI6 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, in the interests of national security, for the purposes of the prevention or detection of serious crime or for the purpose of any criminal proceedings.

101. According to section 1 of the ISA, the functions of MI6 are to obtain and provide information relating to the actions or intentions of persons outside the British Islands; and to perform other tasks relating to the actions or intentions of such persons. Those functions may only be exercised in the interests of national security, with particular reference to the State’s defence and foreign policies; in the interests of the economic well-being of the United Kingdom; or in support of the prevention or detection of serious crime.

(c) GCHQ

102. Section 4 of the ISA provides that it is the duty of the Director of GCHQ, who is appointed by the Secretary of State, to ensure that there are arrangements for securing that it obtains no information 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.

103. According to section 3 of the ISA, one of the functions of GCHQ is 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. This function is exercisable only in the interests of national security, with particular reference to the State's defence and foreign policies; 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 in support of the prevention or detection of serious crime.

(d) Counter-Terrorism Act 2008

104. Section 19 of the Counter-Terrorism Act 2008 allows the disclosure of information to any of the intelligence services for the purpose of the exercise of any of their functions. Information obtained by an intelligence service in connection with the exercise of its functions may be used by that service in connection with the exercise of any of its other functions.

105. Information obtained by MI5 may be disclosed for the purpose of the proper discharge of its functions, for the purpose of the prevention or detection of serious crime, or for the purpose of any criminal proceedings. Information obtained by MI6 may be disclosed for the purpose of the proper discharge of its functions, in the interests of national security, for the purpose of the prevention or detection of serious crime, or for the purpose of any criminal proceedings. Information obtained by GCHQ may be disclosed by it for the purpose of the proper discharge of its functions or for the purpose of any criminal proceedings.

(e) The Data Protection Act 1998 ("DPA")

106. The DPA is the legislation transposing into United Kingdom law Directive 95/46/EC on the protection of personal data. Each of the intelligence services is a "data controller" for the purposes of the DPA and, as such, they are required to comply – subject to exemption by Ministerial certificate – with the data protection principles in Part 1 of Schedule 1, including:

"(5) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes ...

and

"(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."

(f) The Official Secrets Act 1989 ("OSA")

107. A member of the intelligence services commits an offence under section 1(1) of the OSA if he discloses, without lawful authority, any

information, document or other article relating to security or intelligence which is in his possession by virtue of his position as a member of those services.

(g) The Human Rights Act 1998 (“HRA”)

108. Pursuant to section 6 of the HRA, it is unlawful for a public authority to act in a way which is incompatible with a Convention right.

3. The Interception of Communications Code of Practice

109. Following the *Liberty* proceedings, the information contained in the 9 October disclosure was incorporated into the IC Code of Practice:

“12. RULES FOR REQUESTING AND HANDLING UNANALYSED INTERCEPTED COMMUNICATIONS FROM A FOREIGN GOVERNMENT

Application of this chapter

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 an intercepting agency to the government of a country or territory outside the UK for unanalysed intercepted communications (and associated communications data), otherwise than in accordance with an international mutual assistance agreement, if either:

- A relevant interception warrant under RIPA has already been issued by the Secretary of State, the assistance of the foreign government is necessary to obtain the particular communications because they cannot be obtained under the relevant RIPA interception warrant and it is necessary and proportionate for the intercepting agency to obtain those communications; or
- Making the request for the particular communications 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 intercepting agency 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

40 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

“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.

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 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.

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.”

C. Acquisition of communications data

1. Chapter II of RIPA

110. Chapter II of Part 1 of RIPA sets out the framework under which public authorities may acquire communications data from CSPs.

111. Pursuant to section 22, authorisation for the acquisition of communications data from CSPs is granted by a “designated person”, being a person holding such office, rank or position with relevant public authorities as are prescribed by an order made by the Secretary of State. The designated person may either grant authorisation for persons within the same “relevant public authority” as himself to “engage in conduct to which this Chapter applies” (authorisation under section 22(3)), or he may, by notice to the CSP, require it to either disclose data already in its possession, or to obtain and disclose data (notice under section 22(4)). For the purposes of section 22(3), “relevant public authorities” includes a police force, the National Crime Agency, Her Majesty’s Revenue and Customs, any of the intelligence services, and any such public authority as may be specified by an order made by the Secretary of State.

112. Section 22(2) further provides that the designated person may only grant an authorisation under section 22(3) or give a notice under section 22(4) if he believes it is necessary for one of the following grounds:

BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT 41

- “(a) in the interests of national security;
- (b) for the purpose of preventing or detecting crime or of preventing disorder;
- (c) in the interests of the economic well-being of the United Kingdom;
- (d) in the interests of public safety;
- (e) for the purpose of protecting public health;
- (f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;
- (g) for the purpose, in an emergency, of preventing death or injury or any damage to a person’s physical or mental health, or of mitigating any injury or damage to a person’s physical or mental health; or
- (h) for any purpose (not falling within paragraphs (a) to (g)) which is specified for the purposes of this subsection by an order made by the Secretary of State.”

113. He must also believe that obtaining the data is proportionate to what is sought to be achieved.

114. Section 23 requires that the authorisation or notice be granted in writing or, if not, in a manner which produces a record of it having been granted. It must also describe the conduct authorised, the communications data to be obtained or disclosed, set out the grounds on which it is believed necessary to grant the authorisation or give the notice, and specify the office, rank or position of the person giving the authorisation.

115. Authorisations under section 22(3) and notices under section 22(4) last for one month, but may be renewed at any time before the expiry of that period.

116. The person who has given a notice under section 22(4) may cancel it if he is satisfied that it is no longer necessary for one of the specified grounds, or it is no longer proportionate to what is sought to be achieved.

2. The Acquisition and Disclosure of Communications Data: Code of Practice

117. The Acquisition and Disclosure of Communications Data: Code of Practice, issued under section 71 RIPA and last updated in 2015, provides, as relevant:

“1 INTRODUCTION

1.1. This code of practice relates to the powers and duties conferred or imposed under Chapter II of Part I of the Regulation of Investigatory Powers Act 2000 (‘RIPA’). It provides guidance on the procedures to be followed when acquisition of communications data takes place under those provisions. This version of the code replaces all previous versions of the code.

1.2. This code applies to relevant public authorities within the meaning of RIPA: those listed in section 25 or specified in orders made by the Secretary of State under section 25.

42 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

1.3. Relevant public authorities for the purposes of Chapter II of Part I of RIPA ('Chapter II') should not:

- use other statutory powers to obtain communications data from a postal or telecommunications operator unless that power provides explicitly for obtaining communications data, or is conferred by a warrant or order issued by the Secretary of State or a person holding judicial office; or
- require, or invite, any postal or telecommunications operator to disclose communications data by exercising any exemption to the principle of non-disclosure of communications data under the Data Protection Act 1998 ('the DPA').

...

1.7. The exercise of powers and duties under Chapter II is kept under review by the Interception of Communications Commissioner ('the Commissioner') appointed under section 57 of RIPA and by his inspectors who work from the Interception of Communications Commissioner's Office (IOCCO).

...

2 GENERAL EXTENT OF POWERS

Scope of Powers, Necessity and Proportionality

2.1. The acquisition of communications data under RIPA will be a justifiable interference with an individual's human rights under Articles 8 and, in certain circumstances, 10 of the European Convention on Human Rights only if the conduct being authorised or required to take place is both necessary and proportionate and in accordance with law.

2.2. RIPA stipulates that conduct to be authorised or required must be necessary for one or more of the purposes set out in section 22(2) of RIPA:

- in the interests of national security;
- for the purpose of preventing or detecting crime or of preventing disorder;
- in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security;
- in the interests of public safety;
- for the purpose of protecting public health;
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;
- for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health;
- to assist investigations into alleged miscarriages of justice;
- for the purpose of assisting in identifying any person who has died otherwise than as a result of crime or who is unable to identify himself because of a physical or mental condition, other than one resulting from crime (such as a natural disaster or an accident);

- in relation a person who has died or is unable to identify himself, for the purpose of obtaining information about the next of kin or other connected persons of such a person or about the reason for their death or condition; and
- for the purpose of exercising functions relating to the regulation of financial services and markets or to financial stability.

2.3. The purposes for which some public authorities may seek to acquire communications data are restricted by order. The designated person may only consider necessity on grounds open to their public authority and only in relation to matters that are the statutory or administrative function of their respective public authority. The purposes noted above should only be used by a public authority in relation to the specific (and often specialist) offences or conduct that it has been given the statutory function to investigate.

2.4. There is a further restriction upon the acquisition of communications data for the following purposes:

- in the interests of public safety;
- for the purpose of protecting public health; and
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department.

Only communications data within the meaning of section 21(4)(c) of RIPA [being subscriber information] may be acquired for these purposes and only by those public authorities permitted by order to acquire communications data for one or more of those purposes.

2.5. When a public authority wishes to acquire communications data, the designated person must believe that the acquisition, in the form of an authorisation or notice, is necessary. He or she must also believe that conduct to be proportionate to what is sought to be achieved by obtaining the specified communications data – that the conduct is no more than is required in the circumstances. This involves balancing the extent of the interference with an individual's rights and freedoms against a specific benefit to the investigation or operation being undertaken by a relevant public authority in the public interest.

2.6. As well as consideration of the rights of the individual under investigation, consideration must also be given to any actual or potential infringement of the privacy and other rights of individuals who are not the subject of the investigation or operation. An application for the acquisition of communications data should draw attention to any circumstances which give rise to significant collateral intrusion.

2.7. Particular consideration must also be given, when pertinent, to the right to freedom of expression.

2.8. Taking all these considerations into account in a particular case, an interference with the rights of an individual may still not be justified because the adverse impact on the rights of another individual or group of individuals is too severe.

2.9. Any conduct where the interference is excessive in relation to the aims of the investigation or operation, or is in any way arbitrary, will not be proportionate.

2.10. Before public authorities can request communications data, authorisation must be given by the designated person in the relevant authority. A designated person is someone holding a prescribed office, rank or position within a relevant public

44 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

authority that has been designated for the purpose of acquiring communications data by order.

2.11. The relevant public authorities for Chapter II are set out in section 25(1). They are:

- a police force (as defined in section 81(1) of RIPA);
- the National Crime Agency;
- HM Revenue and Customs;
- the Security Service;
- the Secret Intelligence Service; and
- the Government Communications Headquarters.

These and additional relevant public authorities are listed in the Regulation of Investigatory Powers (Communications Data) Order 201033 and any similar future orders made under section 25 of the Act.

Communications Data

2.12. The code covers any conduct relating to the exercise of powers and duties under Chapter II of Part I of RIPA to acquire or disclose communications data. Communications data is defined in section 21(4) of RIPA.

2.13. The term ‘communications data’ embraces the ‘who’, ‘when’, ‘where’, and ‘how’ of a communication but not the content, not what was said or written.

2.14. It includes the manner in which, and by what method, a person or machine communicates with another person or machine. It excludes what they say or what data they pass on within a communication including text, audio and video (with the exception of traffic data to establish another communication such as that created from the use of calling cards, redirection services, or in the commission of ‘dial through’ fraud and other crimes, where data is passed on to activate communications apparatus in order to obtain communications services fraudulently).

2.15. It can include the address on an envelope, the time and duration of a communication, the telephone number or email address of the originator and recipient, and sometimes the location of the device from which the communication was made. It can also include data relating to unsuccessful call attempts i.e. when the person being dialled does not answer the call, but where the network has been able to connect it successfully. It does not include data relating to an unconnected call i.e. when a call is placed, but the network is unable to carry it to its intended recipient. It covers electronic communications (not just voice telephony) and also includes postal services.

2.16. Communications data is generated, held or obtained in the provision, delivery and maintenance of communications services, those being postal services or telecommunications services. DRIPA clarified the definition of telecommunications service in section 2 of RIPA to make explicit that provision of access to systems for the creation, management or storage of communications is included in the provision of a service.

2.17. ‘Communications service providers’ may therefore include those persons who provide services where customers, guests or members of the public are provided with access to communications services that are ancillary to the provision of another service, for example in hotels, restaurants, libraries and airport lounges.

2.18. In circumstances where it is impractical for the data to be acquired from, or disclosed by, the service provider, or where there are security implications in doing so, the data may be sought from the CSP which provides the communications service offered by such hotels, restaurants, libraries and airport lounges. Equally, circumstances may necessitate the acquisition of further communications data for example, where a hotel is in possession of data identifying specific telephone calls originating from a particular guest room.

2.19. Consultation with the public authority's Single Point of Contact (SPoC) will determine the most appropriate plan for acquiring data where the provision of a communication service engages a number of providers, though it is the designated person who ultimately decides which of the CSPs should be given a notice. With the proliferation of modern communications media, including mobile telephony, internet communications, and social networks, and given that one individual can use many different forms of communications, the knowledge and experience of the SPoC in providing advice and guidance to the designated person is significant in ensuring appropriateness of any action taken to acquire the data necessary for an investigation. If a CSP, having been given a notice, believes that in future another CSP is better placed to respond, they should approach the authority to inform them of their view after disclosing the relevant data that they hold.

2.20. Any conduct to determine the CSP that holds, or may hold, specific communications data is not conduct to which the provisions of Chapter II apply. This includes, for example, establishing from information available to the public or, where necessary, from a service provider which provider makes available a specific service, such as a particular telephone number or an internet protocol address.

2.21. Communications data is defined as:

- traffic data (as defined by sections 21(4)(a) and 21(6) of RIPA) – this is data that is or has been comprised in or attached to a communication for the purpose of its transmission (see section starting at paragraph 2.24 of this code for further detail);
- service use information (as defined by section 21(4)(b) of RIPA) – this is the data relating to the use made by a person of a communications service (see section starting at paragraph 2.28 of this code for further detail); and
- subscriber information (as defined by section 21(4)(c) of RIPA) – this relates to information held or obtained by a CSP about persons to whom the CSP provides or has provided a communications services. Those persons will include people who are subscribers to a communications service without necessarily using that service and persons who use a communications service without necessarily subscribing to it (see section starting at paragraph 2.30 of this code for further detail).

2.22. The data available on individuals, and the level of intrusion, differs between the categories of data. The public authorities which can acquire the data and, in some cases, the level of seniority of the designated person differ according to the categories of data in question.

...

Traffic Data

2.24. RIPA defines certain communications data as 'traffic data' in sections 21(4)(a) and 21(6) of RIPA. This is data that is or has been comprised in or

46 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

attached to a communication for the purpose of transmitting the communication and which ‘in relation to any communication’:

- identifies, or appears to identify, any person, apparatus or location to or from which a communication is or may be transmitted;
- identifies or selects, or appears to identify or select, transmission apparatus;
- comprises signals that activate apparatus used, wholly or partially, for the transmission of any communication (such as data generated in the use of carrier pre-select or redirect communication services or data generated in the commission of, what is known as, ‘dial through’ fraud); or
- identifies data as data comprised in, or attached to, a communication. This includes data which is found at the beginning of each packet in a packet switched network that indicates which communications data attaches to which communication.

2.25. Traffic data includes data identifying a computer file or a computer program to which access has been obtained, or which has been run, by means of the communication – but only to the extent that the file or program is identified by reference to the apparatus in which the file or program is stored. In relation to internet communications, this means traffic data stops at the apparatus within which files or programs are stored, so that traffic data may identify a server or domain name (web site) but not a web page. For example, the fact that a subject of interest has visited pages at <http://www.gov.uk/> can be acquired as communications traffic data (if available from the CSP), whereas that a specific webpage that was visited is <http://www.gov.uk/government/collections/ripa-forms-2> may not be acquired as communications data (as it would be content).

2.26. Examples of traffic data, within the definition in section 21(6), include:

- information tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records);
- information identifying the location of apparatus when a communication is, has been or may be made or received (such as the location of a mobile phone);
- information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or attached to the communication;
- routing information identifying apparatus through which a communication is or has been transmitted (for example, dynamic IP address allocation, file transfer logs and e mail headers – to the extent that content of a communication, such as the subject line of an e mail, is not disclosed);
- web browsing information to the extent that only a host machine, server, domain name or IP address is disclosed;
- anything, such as addresses or markings, written on the outside of a postal item (such as a letter, packet or parcel) that is in transmission and which shows the item’s postal routing;
- records of correspondence checks comprising details of traffic data from postal items in transmission to a specific address; and

- online tracking of communications (including postal items and parcels).

...

Service Use Information

2.28. Data relating to the use made by any person of a postal or telecommunications service, or any part of it, is widely known as ‘service use information’ and falls within section 21(4)(b) of RIPA.

2.29. Service use information is, or can be, routinely made available by a CSP to the person who uses or subscribes to the service to show the use of a service or services and to account for service charges over a given period of time. Examples of data within the definition at section 21(4)(b) include:

- itemised telephone call records (numbers called);
- itemised records of connections to internet services;
- itemised timing and duration of service usage (calls and/or connections);
- information about amounts of data downloaded and/or uploaded;
- information about the use made of services which the user is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services;
- information about the use of forwarding/redirection services;
- information about selection of preferential numbers or discount calls; and
- records of postal items, such as records of registered post, recorded or special delivery postal items, records of parcel consignment, delivery and collection.

Subscriber Information

2.30. The third type of communications data, widely known as ‘subscriber information’, is set out in section 21(4)(c) of RIPA. This relates to information held or obtained by a CSP about persons to whom the CSP provides or has provided a communications service. Those persons will include people who are subscribers to a communications service without necessarily using that service and persons who use a communications service without necessarily subscribing to it.

2.31. Examples of data within the definition at section 21(4)(c) include:

- ‘subscriber checks’ (also known as ‘reverse look ups’) such as “who is the subscriber of phone number 01632 960 224?”, “who is the account holder of e-mail account example@example.co.uk?” or “who is entitled to post to web space www.example.co.uk?”;
- information about the subscriber to a PO Box number or a Postage Paid Impression used on bulk mailings;
- information about the provision to a subscriber or account holder of forwarding/redirection services, including delivery and forwarding addresses;
- subscribers’ or account holders’ account information, including names and addresses for installation, and billing including payment method(s), details of payments;

48 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

- information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services, and potentially static IP addresses;
- information about apparatus used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes; and
- information provided by a subscriber or account holder to a CSP, such as demographic information or sign-up data (to the extent that information, such as a password, giving access to the content of any stored communications is not disclosed save where the requirement for such information is necessary in the interests of national security).

...

2.35. Additional types of data may fall into the category of subscriber information, as communications services have developed and broadened, for example where a CSP chooses to collect information about the devices used by their customers. Prior to the acquisition of data which does not fall into the illustrative list of traditional subscriber information above, specific consideration should be given to whether it is particularly sensitive or intrusive, in order to ensure that such a request is still necessary and proportionate, and compliant with Chapter II.

Further Guidance on Necessity and Proportionality

2.36. Training regarding necessity and proportionality should be made available to all those who participate in the acquisition and disclosure of communications data.

Necessity

2.37. In order to justify that an application is necessary, the application needs as a minimum to cover three main points:

- the event under investigation, such as a crime or vulnerable missing person;
- the person, such as a suspect, witness or missing person, and how they are linked to the event; and
- the communications data, such as a telephone number or IP address, and how this data is related to the person and the event.

2.38. Necessity should be a short explanation of the event, the person and the communications data and how these three link together. The application must establish the link between the three aspects to be able to demonstrate the acquisition of communications data is necessary for the statutory purpose specified.

Proportionality

2.39. Applications should include an outline of how obtaining the data will benefit the investigation or operation. If more than one item of data is being sought, the relevance of the additional data should be explained.

2.40. This should include explaining how the level of intrusion is justified when taking into consideration the benefit the data will give to the investigation. This justification should include confirmation that relevant less intrusive investigations have already been undertaken where possible. For example, the subscriber details of a

phone number may be obtainable from a phone book or other publically available sources.

2.41. The relevance of any time periods requested must be explained, outlining how these periods are proportionate to the event under investigation.

2.42. An examination of the proportionality of the application should particularly include a consideration of the rights (particularly to privacy and, in relevant cases, freedom of expression) of the individual and a balancing of these rights against the benefit to the investigation.

2.43. Collateral intrusion is the obtaining of any information relating to individuals other than the subject(s) of the investigation. Consideration of collateral intrusion forms part of the proportionality considerations, and becomes increasingly relevant when applying for traffic data or service use data. Applications should include details of what collateral intrusion may occur and how the time periods requested impact on the collateral intrusion. When there are no meaningful collateral intrusion risks, such as when applying for subscriber details of the person under investigation, the absence of collateral intrusion should be noted.

2.44. An examination of the proportionality of the application should also involve a consideration of possible unintended consequences and, when, relevant this should be noted. Unintended consequences of an application are outcomes that are not intended by the application.

2.45. Unintended consequences are more likely in more complicated requests for traffic data or in applications for the data of those in professions with duties of confidentiality. For example, if a journalist is a victim of crime, applications for service use data related to that journalist's phone number as part of the criminal investigation may also return some phone numbers of that journalist's sources, with unintended impact on freedom of expression. Such an application may still be necessary and proportionate but the risk of unintended consequences should be considered. The special considerations that arise in such cases are discussed further in the section on "Communications data involving certain professions".

3 GENERAL RULES ON THE GRANTING OF AUTHORISATIONS AND GIVING OF NOTICES

3.1. Acquisition of communications data under RIPA involves four roles within a relevant public authority:

- the applicant;
- the designated person;
- the single point of contact; and
- the senior responsible officer

3.2. RIPA provides two alternative means for acquiring communications data, by way of:

- an authorisation under section 22(3); or
- a notice under section 22(4).

An authorisation granted to a member of a public authority permits that person to engage in conduct relating to the acquisition and disclosure of communications data under Part I Chapter II of RIPA. A notice given to a postal or telecommunications operator requires it to disclose the relevant communications data held by it to a public

authority, or to obtain and disclose the data, when it is reasonably practicable for them to do so. Both authorisations and notices are explained in more detail within this chapter.

The applicant

3.3. The applicant is a person involved in conducting an investigation or operation for a relevant public authority who makes an application in writing or electronically for the acquisition of communications data. The applicant completes an application form, setting out for consideration by the designated person, the necessity and proportionality of a specific requirement for acquiring communications data.

3.4. An application may be made orally in exceptional circumstances, but a record of that application must be made in writing or electronically as soon as possible, and certainly within one working day (paragraphs 3.65 - 3.71 provide more detail on urgent procedures).

3.5. An application – the original or a copy of which must be retained by the SPoC within the public authority – must:

- include the name (or designation) and the office, rank or position held by the person making the application;
- include a unique reference number;
- include the operation name (if applicable) to which the application relates;
- specify the purpose for which the data is required, by reference to a statutory purpose under 22(2) of RIPA;
- describe the communications data required, specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s);
- describe whether the communications data relates to a victim, a witness, a complainant, a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation;
- explain why the acquisition of that data is considered necessary and proportionate to what is sought to be achieved by acquiring it;
- consider and, where appropriate, describe any meaningful collateral intrusion – the extent to which the rights of any individual not under investigation may be infringed and why that intrusion is justified in the circumstances;
- consider and, where appropriate, describe any possible unintended consequences of the application; and
- identify and explain the time scale within which the data is required.

3.6. The application should record subsequently whether it was approved by a designated person, by whom and when that decision was made. If approved, the application form should, to the extent necessary, be cross-referenced to any authorisation granted or notice given.

The designated person

3.7. The designated person is a person holding a prescribed office in a relevant public authority. It is the designated person's responsibility to consider the application and record their considerations at the time (or as soon as is reasonably practicable) in

writing or electronically. If the designated person believes the acquisition of communications data is necessary and proportionate in the specific circumstances, an authorisation is granted or a notice is given.

3.8. Individuals who undertake the role of a designated person must have current working knowledge of human rights principles and legislation, specifically those of necessity and proportionality, and how they apply to the acquisition of communications data under Chapter II and this code.

3.9. When considering proportionality, the designated person should apply particular consideration to unintended consequences. The seniority, experience and training of the designated person provides them with a particular opportunity to consider possible unintended consequences.

3.10. Designated persons must ensure that they grant authorisations or give notices only for purposes and only in respect of types of communications data that a designated person of their office, rank or position in the relevant public authority may grant or give.

3.11. The designated person shall assess the necessity for any conduct to acquire or obtain communications data taking account of any advice provided by the single point of contact (SPoC).

3.12. Designated persons must be independent from operations and investigations when granting authorisations or giving notices related to those operations.

3.13. Except where it is necessary to act urgently, in circumstances where a public authority is not able to call upon the services of a designated person who is independent from the investigation or operation, the Senior Responsible Officer must inform the Interception of Communications Commissioner of the circumstances and reasons (noting the relevant designated persons who, in these circumstances, will not be independent). These may include:

- small specialist criminal investigation departments within public authorities which are not law enforcement or intelligence agencies; and
- public authorities which have on-going operations or investigations immediately impacting on national security issues and are therefore not able to call upon a designated person who is independent from their operations and investigations.

3.14. In all circumstances where public authorities use designated persons who are not independent from an operation or investigation this must be notified to the Commissioner at the next inspection. The details of the public authorities and the reasons such measures are being undertaken may be published and included in the Commissioner's report.

3.15. Where a designated person is not independent from the investigation or operation their involvement and their justification for undertaking the role of the designated person must be explicit in their recorded considerations.

3.16. Particular care must be taken by designated persons when considering any application to obtain communications data to identify apparatus (such as a mobile telephone) at or within a location or locations and at or between times on a given date or dates where the identity of the apparatus is unknown. Unless the application is based on information that the apparatus was used or was likely to have been used in a particular location or locations at a particular time or times it will, in practice, be rare

that any conduct to obtain communications data will be proportionate or the collateral intrusion justified.

...

The single point of contact

3.19. The single point of contact (SPoC) is an accredited individual trained to facilitate lawful acquisition of communications data and effective co-operation between a public authority and CSPs. Despite the name, in practice many organisations will have multiple SPoCs, working together. To become accredited an individual must complete a course of training appropriate for the role of a SPoC and have been issued the relevant SPoC authentication identifier. SPoCs in public authorities should be security cleared in accordance with their own organisation's requirements. Details of all accredited individuals are available to CSPs for authentication purposes.

3.20. Communications data should be treated as information with a classification of OFFICIAL and a caveat of SENSITIVE, though it may be classified higher if appropriate. When handling, processing, and distributing such information, SPoCs must comply with local security policies and operating procedures. The SENSITIVE caveat is for OFFICIAL information that is subject to 'need to know' controls so that only authorised personnel can have access to the material. This does not preclude, for example, the disclosure of material or the use of this material as evidence in open court when required. Rather, the classification and caveat of OFFICIAL - SENSITIVE makes clear that communications data must be treated with care, noting the impact on the rights to privacy and, where appropriate, freedom of expression of the subjects of interest and, depending on the data, possibly some of their communications contacts. Communications data acquired by public authorities must also be stored and handled in accordance with duties under the Data Protection Act.

3.21. An accredited SPoC promotes efficiency and good practice in ensuring only practical and lawful requirements for communications data are undertaken. This encourages the public authority to regulate itself. The SPoC provides objective judgement and advice to both the applicant and the designated person. In this way the SPoC provides a 'guardian and gatekeeper' function ensuring that public authorities act in an informed and lawful manner.

3.22. The SPoC should be in a position to:

- engage proactively with applicants to develop strategies to obtain communications data and use it effectively in support of operations or investigations;
- assess whether the acquisition of specific communications data from a CSP is reasonably practical or whether the specific data required is inextricably linked to other data;
- advise applicants on the most appropriate methodology for acquisition of data where the data sought engages a number of CSPs;
- advise applicants and designated persons on the interpretation of RIPA, particularly whether an authorisation or notice is appropriate;
- provide assurance to designated persons that authorisations and notices are lawful under RIPA and free from errors;

- consider and, where appropriate, provide advice to the designated person on possible unintended consequences of the application;
- provide assurance to CSPs that authorisations and notices are authentic and lawful;
- assess whether communications data disclosed by a CSP in response to a notice fulfils the requirement of the notice;
- assess whether communications data obtained by means of an authorisation fulfils the requirement of the authorisation; and
- assess any cost and resource implications to both the public authority and the CSP of data requirements.

3.23. The SPoC would normally be the person who takes receipt of any communications data acquired from a CSP (see paragraphs 3.33 and 3.49) and would normally be responsible for its dissemination to the applicant.

3.24. Public authorities unable to call upon the services of an accredited SPoC should not undertake the acquisition of communications data. Nonetheless, in the course of a joint investigation between authority A with no SPoC and authority B with RIPA communications data acquisition powers, authority B may, where necessary and proportionate, acquire communications data under RIPA to further the joint investigation.

3.25. In circumstances where a CSP is approached by a person who cannot be authenticated as an accredited individual and who seeks to obtain data under the provisions of RIPA, the CSP may refuse to comply with any apparent requirement for disclosure of data until confirmation of both the person's accreditation and their SPoC authentication identifier is obtained from the Home Office.

3.26. For each individual application, the roles of SPoC and designated persons will normally be carried out by two persons. In exceptional cases, such as those covered under the urgent oral procedure or, on rare occasions, for security reasons, both roles may be carried out by the same person. One person may, in separate applications, carry out the roles of either the SPoC or the designated person.

3.27. For each individual application, the roles of SPOC and Applicant will also normally be carried out by two persons. In exceptional cases, such as those covered under the urgent oral procedure or, on rare occasions, for security reasons, both roles may be carried out by the same person. One person may, in separate applications, carry out the roles of either the SPOC or the Applicant.

3.28. The same person must never be both the applicant and the designated person. Clearly, therefore, the same person should never be an applicant, a designated person and a SPoC.

3.29. Where a public authority seeks to obtain communications data using provisions providing explicitly for the obtaining of communications data (other than Chapter II of Part I of RIPA) or using statutory powers conferred by a warrant or order issued by the Secretary of State or a person holding judicial office, the SPoC should be engaged in the process of obtaining the data to ensure effective co-operation between the public authority and the CSP.

3.30. Occasionally public authorities will wish to request data from CSPs that is neither communications data nor the content of communications. Given the training

54 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

undertaken by a SPoC and the on-going nature of a SPoC's engagement with CSPs, it is good practice to engage the SPoC to liaise with the CSP on such requests.

The senior responsible officer

3.31. Within every relevant public authority a senior responsible officer must be responsible for:

- the integrity of the process in place within the public authority to acquire communications data;
- compliance with Chapter II of Part I of RIPA and with this code;
- oversight of the reporting of errors to IOCCO and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- engagement with the IOCCO inspectors when they conduct their inspections; and
- where necessary, oversight of the implementation of post-inspection action plans approved by the Commissioner.

Authorisations

3.32. An authorisation provides for persons within a public authority to engage in specific conduct, relating to a postal service or telecommunications system, to obtain communications data.

3.33. Any designated person in a public authority may only authorise persons working in the same public authority to engage in specific conduct, such as requesting the data via secure auditable communications data acquisition systems. This will normally be the public authority's SPoC, though local authorities must now use the National Anti-Fraud Network (see later in this chapter for more details).

3.34. The decision of a designated person whether to grant an authorisation shall be based upon information presented to them in an application.

3.35. An authorisation may be appropriate where:

- a CSP is not capable of obtaining or disclosing the communications data;
- there is an agreement in place between a public authority and a CSP relating to appropriate mechanisms for disclosure of communications data; or
- a designated person considers there is a requirement to identify a person to whom a service is provided but a CSP has yet to be conclusively determined as the holder of the communications data.

3.36. An authorisation is not served upon a CSP, although there may be circumstances where a CSP may require or may be given an assurance that conduct being, or to be, undertaken is lawful. That assurance may be given by disclosing details of the authorisation or the authorisation itself.

3.37. An authorisation – the original or a copy of which must be retained by the SPoC within the public authority – must:

- be granted in writing or, if not, in a manner that produces a record of it having been granted;

BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT 55

- describe the conduct which is authorised and describe the communications data to be acquired by that conduct specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s);
- specify the purpose for which the conduct is authorised, by reference to a statutory purpose under section 22(2) of RIPA;
- specify the office, rank or position held by the designated person granting the authorisation. The designated person should also record their name (or designation) on any authorisation they grant; and
- record the date and, when appropriate to do so, the time when the authorisation was granted by the designated person.

...

3.40. At the time of giving a notice or granting an authorisation to obtain specific traffic data or service use data, a designated person may also authorise, to the extent necessary and proportionate at that time, the consequential acquisition of specific subscriber information relating to the traffic data or service use data to be obtained. This is relevant where there is a necessary and proportionate requirement to identify with whom a person has been in communication, for example:

- to identify with whom a victim was in contact, within a specified period, prior to their murder;
- to identify, where the target of an investigation or operation has been observed to make several calls from a public pay phone, the recipient of those calls;
- to identify a person making unlawful and unwarranted demands (as in the case of kidnap, extortion and blackmail demands and threats of violence); and
- where a victim or a witness has identified a specific communication or communications and corroboration of facts may reveal a potential offender or other witness.

3.41. At the time of giving a notice or granting an authorisation to obtain specific traffic data, a designated person may also authorise, to the extent necessary and proportionate at that time, the consequential acquisition of traffic data or service use information. This is relevant where there is a necessary and proportionate requirement to identify a person from the traffic data to be acquired, and the means to do so requires the CSP or another CSP to query their traffic data or service use information, for example:

- the CSP does not collect information about the customer within their customer information system but retains it in its original form as traffic data (such as a MAC or IMEI or an IP address); or
- where evidence or intelligence indicates there are several CSPs involved in routing a communication and there is a requirement to establish the recipient of the communication.

3.42. It is the duty of the senior responsible officer to ensure that the designated person, applicant or other person makes available to the SPoC such information as the senior responsible officer thinks necessary to ensure the integrity of any requirements for the acquisition of subscriber information to be obtained directly upon the

acquisition or disclosure of any traffic data or service use data, and their compliance with Chapter II and with this code.

Notices

3.43. The giving of a notice is appropriate where a CSP is able to retrieve or obtain specific data, and to disclose that data, unless the grant of an authorisation is more appropriate. A notice may require a CSP to obtain any communications data, if that data is not already in its possession.

3.44. The decision of a designated person whether to give a notice shall be based on information presented to them in an application.

3.45. The ‘giving of a notice’ means the point at which a designated person determines that a notice should be given to a CSP. In practice, once the designated person has determined that a notice should be given, it will be served upon a CSP in writing or, in an urgent situation, communicated to the CSP orally.

3.46. The notice should contain enough information to allow the CSP to comply with the requirements of the notice.

3.47. A notice – the original or a copy of which must be retained by the SPoC within the public authority – must:

- be given in writing or, if not, in a manner that produces a record, within the public authority, of its having been given;
- include a unique reference number and also identify the public authority;
- specify the purpose for which the notice has been given, by reference to a statutory purpose under 22(2) of RIPA;
- describe the communications data to be obtained or disclosed under the notice specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s);
- include an explanation that compliance with the notice is a requirement of RIPA;
- specify the office, rank or position held by the designated person giving the notice. The name (or designation) of the designated person giving the notice should also be recorded;
- specify the manner in which the data should be disclosed. The notice should contain sufficient information including the contact details of the SPoC to enable a CSP to confirm the notice is authentic and lawful;
- record the date and, when appropriate to do so, the time when the notice was given by the designated person; and
- where appropriate, provide an indication of any urgency or time within which the CSP is requested to comply with the requirements of the notice.

3.48. A notice must not place a CSP under a duty to do anything which it is not reasonably practicable for the CSP to do. SPoCs should be mindful of the need to draft notices to ensure the description of the required data corresponds with the ways in which the CSP processes, retains and retrieves its data for lawful disclosure. CSPs cannot necessarily or reasonably edit or adapt their systems to take account of every possible variation of what may be specified in notices.

3.49. In giving notice a designated person may only require a CSP to disclose the communications data to the designated person or to a specified person working within the same public authority. This will normally be the public authority's SPoC.

3.50. Ordinarily the CSP should disclose, in writing or electronically, the communications data to which a notice relates not later than the end of the period of ten working days from the date the notice is served upon the CSP.

Duration of authorisations and notices

3.51. An authorisation or notice becomes valid on the date upon which authorisation is granted or notice given. It is then valid for a maximum of one month. This means the conduct authorised should have been commenced or the notice served within that month.

3.52. All authorisations and notices should refer to the acquisition or disclosure of data relating to a specific date(s) or period(s). Any period should be clearly indicated in the authorisation or notice. The start date and end date should be given, and where a precise start and end time are relevant these must be specified. Where the data to be acquired or disclosed is specified as 'current', the relevant date should be taken to be the date on which the authorisation was granted or the notice given by the designated person. There can be circumstances when the relevant date or period cannot be specified other than 'the last transaction' or 'the most recent use of the service'.

3.53. Where an authorisation or a notice relates to the acquisition or obtaining of specific data that will or may be generated in the future, the future period is restricted to no more than one month from the date upon which the authorisation was granted or the notice given.

3.54. Designated persons should specify the shortest possible period of time for any authorisation or notice. To do otherwise would impact on the proportionality of the authorisation or notice and impose an unnecessary burden upon the relevant CSP(s).

Renewal of authorisations and notices

3.55. Any valid authorisation or notice may be renewed for a period of up to one month by the grant of a further authorisation or the giving of a further notice. A renewed authorisation or notice takes effect upon the expiry of the authorisation or notice it is renewing.

3.56. Renewal may be appropriate where there is a continuing requirement to acquire or obtain data that will or may be generated in the future. The reasoning for seeking renewal should be set out by an applicant in an addendum to the application upon which the authorisation or notice being renewed was granted or given.

3.57. Where a designated person is granting a further authorisation or giving a further notice to renew an earlier authorisation or notice, the designated person should:

- have considered the reasons why it is necessary and proportionate to continue with the acquisition of the data being generated; and
- record the date and, when appropriate to do so, the time when the authorisation or notice is renewed.

Cancellation of notices and withdrawal of authorisations

3.58. A designated person who has given notice to a CSP under section 22(4) of RIPA shall cancel the notice if, at any time after giving the notice, it is no longer

58 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

necessary for the CSP to comply with the notice or the conduct required by the notice is no longer proportionate to what was sought to be achieved.

3.59. Reporting the cancellation of a notice to a CSP shall be undertaken by the designated person directly or, on that person's behalf, by the public authority's SPoC. Where human rights considerations are such that a notice should be cancelled with immediate effect the designated person or the SPoC will notify the CSP.

3.60. Cancellation of a notice reported to a CSP must:

- be undertaken in writing or, if not, in a manner that produces a record of the notice having been cancelled;
- identify, by reference to its unique reference number, the notice being cancelled; and
- record the date and, when appropriate to do so, the time when the notice was cancelled.

3.61. In cases where the SPoC has initiated the cancellation of a notice and reported the cancellation to the CSP, the designated person must confirm the decision in writing for the SPoC or, if not, in a manner that produces a record of the notice having been cancelled by the designated person. Where the designated person who gave the notice to the CSP is no longer available, this duty should fall on a person who has temporarily or permanently taken over the role of the designated person.

3.62. Similarly where a designated person considers an authorisation should cease to have effect, because the conduct authorised becomes unnecessary or no longer proportionate to what was sought to be achieved, the authorisation must be withdrawn. It may be the case that it is the SPoC or the applicant who is first aware that the authorisation is no longer necessary or proportionate. In such cases the SPoC (having been contacted by the applicant, where appropriate) may cease the authorised conduct, and then inform the designated person who granted the authorisation.

3.63. Withdrawal of an authorisation should:

- be undertaken in writing or, if not, in a manner that produces a record of it having been withdrawn;
- identify, by reference to its unique reference number, the authorisation being withdrawn;
- record the date and, when appropriate to do so, the time when the authorisation was cancelled; and
- record the name and the office, rank or position held by the designated person informed of the withdrawal of the authorisation.

3.64. When it is appropriate to do so, a CSP should be advised of the withdrawal of an authorisation, for example where details of an authorisation have been disclosed to a CSP.

Urgent oral giving of notice or grant of authorisation

3.65. In exceptionally urgent circumstances, an application for the giving of a notice or the grant of an authorisation may be made by an applicant, approved by a designated person and either notice given to a CSP or an authorisation granted orally. Circumstances in which an oral notice or authorisation may be appropriate include:

- an immediate threat of loss of human life, or for the protection of human life, such that a person's life might be endangered if the application procedure were undertaken in writing from the outset;
- an exceptionally urgent operational requirement where, within no more than 48 hours of the notice being given or the authorisation being granted orally, the acquisition of communications data will directly assist the prevention or detection of the commission of a serious crime and the making of arrests or the seizure of illicit material, and where that operational opportunity will be lost if the application procedure is undertaken in writing from the outset; or
- a credible and immediate threat to national security or a time-critical and unique opportunity to secure, or prevent the loss of, information of vital importance to national security where that threat might be realised, or that opportunity lost, if the application procedure were undertaken in writing from the outset.

3.66. The use of urgent oral process must be justified for each application within an investigation or operation. The fact that any part of an investigation or operation is undertaken urgently must not be taken to mean that all requirements to obtain communications data in connection with that investigation or operation be undertaken using the urgent oral process. It must be clear in each case why it was not possible, in the circumstances, to use the standard, written process.

...

3.69. Written notice must be given to the CSP retrospectively within one working day of the oral notice being given. Failure to do so will constitute an error which may be reported to the Commissioner by the CSP and must be recorded by the public authority (see the section on errors in Chapter 6, Keeping of Records, for more details).

3.70. After the period of urgency, a separate written process must be completed demonstrating the consideration given to the circumstances and the decisions taken. The applicant or the SPoC shall collate details or copies of control room or other operational logs which provide contemporaneous records of the consideration given to the acquisition of data, decision(s) made by the designated person and the actions taken in respect of the decision(s).

3.71. In all cases where urgent oral notice is given or authorisation granted, an explanation of why the urgent process was undertaken must be recorded.

Communications data involving certain professions

3.72. Communications data is not subject to any form of professional privilege – the fact a communication took place does not disclose what was discussed, considered or advised.

3.73. However the degree of interference with an individual's rights and freedoms may be higher where the communications data being sought relates to a person who is a member of a profession that handles privileged or otherwise confidential information (including medical doctors, lawyers, journalists, Members of Parliament, or ministers of religion). It may also be possible to infer an issue of sensitivity from the fact someone has regular contact with, for example, a lawyer or journalist.

3.74. Such situations do not preclude an application being made. However applicants, giving special consideration to necessity and proportionality, must draw

attention to any such circumstances that might lead to an unusual degree of intrusion or infringement of rights and freedoms, particularly regarding privacy and, where it might be engaged, freedom of expression. Particular care must be taken by designated persons when considering such applications, including additional consideration of whether there might be unintended consequences of such applications and whether the public interest is best served by the application.

3.75. Applicants must clearly note in all cases when an application is made for the communications data of those known to be in such professions, including medical doctors, lawyers, journalists, Members of Parliament, or ministers of religion. That such an application has been made must be recorded (see section 6 on keeping of records for more details), including recording the profession, and, at the next inspection, such applications should be flagged to the Interception of Communications Commissioner.

3.76. Issues surrounding the infringement of the right to freedom of expression may arise where a request is made for the communications data of a journalist. There is a strong public interest in protecting a free press and freedom of expression in a democratic society, including the willingness of sources to provide information to journalists anonymously. Where an application is intended to determine the source of journalistic information, there must therefore be an overriding requirement in the public interest, and the guidance at paragraphs 3.78–3.24 should be followed.

3.77. Where the application is for communications data of a journalist, but is not intended to determine the source of journalistic information (for example, where the journalist is a victim of crime or is suspected of committing a crime unrelated to their occupation), there is nevertheless a risk of collateral intrusion into legitimate journalistic sources. In such a case, particular care must therefore be taken to ensure that the application considers whether the intrusion is justified, giving proper consideration to the public interest. The necessity and proportionality assessment also needs to consider whether alternative evidence exists, or whether there are alternative means for obtaining the information being sought. The application should draw attention to these matters.

Applications to determine the source of journalistic information

3.78. In the specific case of an application for communications data, which is made in order to identify a journalist's source, and until such time as there is specific legislation to provide judicial authorisation for such applications, those law enforcement agencies, including the police, National Crime Agency and Her Majesty's Revenue and Customs, in England and Wales with powers under the Police and Criminal Evidence Act 1984 (PACE) must use the procedures of PACE to apply to a court for a production order to obtain this data. Relevant law enforcement agencies in Northern Ireland must apply for a production order under the PACE (Northern Ireland Order) 1989. Law enforcement agencies in Scotland must use the appropriate legislation or common law powers to ensure judicial authorisation for communications data applications to determine journalistic sources.

3.79. Communications data that may be considered to determine journalistic sources includes data relating to:

- journalists' communications addresses;
- the communications addresses of those persons suspected to be a source; and

- communications addresses of persons suspected to be acting as intermediaries between the journalist and the suspected source.

3.80. Each authority must keep a central record of all occasions when such an application has been made, including a record of the considerations.

3.81. This includes that, where the police suspect wrong-doing that includes communications with a journalist, the application must consider properly whether that conduct is criminal and of a sufficiently serious nature for rights to freedom of expression to be interfered with where communications data is to be acquired for the purpose of identifying a journalist's source.

3.82. As described in paragraph 3.29 above, the SPoC should be engaged in this process, to ensure appropriate engagement with the CSPs.

3.83. If and only if there is a believed to be an immediate threat of loss of human life, such that a person's life might be endangered by the delay inherent in the process of judicial authorisation, law enforcement agencies may continue to use the existing internal authorisation process under RIPA. Such applications must be flagged to the Interception of Communications Commissioner as soon as reasonably practicable, as agreed with the Commissioner. If additional communications data is later sought as part of the same investigation, but where a threat to life no longer exists, judicial authorisation must be sought.

3.84. The requirement for judicial oversight does not apply where applications are made for the communications data of those known to be journalists but where the application is not to determine the source of journalistic information. This includes, for example, where the journalist is a victim of crime or is suspected of committing a crime unrelated to their occupation.

Local authority authorisation procedure

3.85. Local authorities must fulfil two additional requirements when acquiring communications data that differ from other public authorities. Firstly, the request must be made through a SPoC at the National Anti-Fraud Network ('NAFN'). Secondly, the request must receive prior judicial approval.

...

6 KEEPING OF RECORDS

Records to be kept by a relevant public authority

6.1. Applications, authorisations, copies of notices, and records of the withdrawal of authorisations and the cancellation of notices, must be retained by the relevant public authority in written or electronic form, and physically attached or cross-referenced where they are associated with each other. The public authority should also keep a record of the date and, when appropriate to do so, the time when each notice or authorisation is given or granted, renewed or cancelled. Records kept by the public authority must be held centrally by the SPoC or in accordance with arrangements previously agreed with the Commissioner.

6.2. These records must be available for inspection by the Commissioner and retained to allow the Investigatory Powers Tribunal, established under Part IV of RIPA, to carry out its functions.

6.3. Where the records contain, or relate to, material obtained directly as a consequence of the execution of an interception warrant, those records must be treated

62 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

in accordance with the safeguards which the Secretary of State has approved in accordance with section 15 of RIPA.

...

6.5. Each relevant public authority must also keep a record of the following information:

A. the number of applications submitted by an applicant to a SPoC requesting the acquisition of communications data (including orally);

B. the number of applications submitted by an applicant to a SPoC requesting the acquisition of communications data (including orally), which were referred back to the applicant for amendment or declined by the SPoC, including the reason for doing so;

C. the number of applications submitted to a designated person for a decision to obtain communications data (including orally), which were approved after due consideration;

D. the number of applications submitted to a designated person for a decision to obtain communications data (including orally), which were referred back to the applicant or rejected after due consideration, including the reason for doing so;

E. the number of notices requiring disclosure of communications data (not including urgent oral applications);

F. the number of authorisations for conduct to acquire communications data (not including urgent oral applications);

G. the number of times an urgent application is approved orally;

H. the number of times an urgent notice is given orally, or an urgent authorisation granted orally, requiring disclosure of communications data;

I. the priority grading of the application for communications data, as set out at paragraph 3.5 and footnote 52 of this code;

J. whether any part of the application relates to a person who is a member of a profession that handles privileged or otherwise confidential information (such as a medical doctor, lawyer, journalist, Member of Parliament, or minister of religion) (and if so, which profession); and

K. the number of items of communications data sought, for each notice given, or authorisation granted (including orally).

6.6. For each item of communications data included within a notice or authorisation, the relevant public authority must also keep a record of the following:

A. the Unique Reference Number (URN) allocated to the application, notice and/or authorisation;

B. the statutory purpose for which the item of communications data is being requested, as set out at section 22(2) of RIPA;

C. where the item of communications data is being requested for the purpose of preventing or detecting crime or of preventing disorder, as set out at section 22(2)(b) of RIPA, the crime type being investigated;

D. whether the item of communications data is traffic data, service use information, or subscriber information, as described at section 21 (4) of RIPA, and Chapter 2 of this code;

E. a description of the type of each item of communications data included in the notice or authorisation;

F. whether the item of communications data relates to a victim, a witness, a complainant, or a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation;

G. the age of the item of communications data. Where the data includes more than one day, the recorded age of data should be the oldest date of the data sought;

H. where an item of data is service use information or traffic data retained by the CSP, an indication of the total number of days of data being sought by means of notice or authorisation; and

I. the CSP from whom the data is being acquired.

6.7. These records must be sent in written or electronic form to the Commissioner, as determined by him. Guidance on record keeping will be issued by IOCCO. Guidance may also be sought by relevant public authorities, CSPs or persons contracted by them to develop or maintain their information technology systems.

6.8. The Interception of Communications Commissioner will not seek to publish statistical information where it appears to him that doing so would be contrary to the public interest, or would be prejudicial to national security.

Records to be kept by a Communications Service Provider

6.9. To assist the Commissioner to carry out his statutory function in relation to Chapter II, CSPs should maintain a record of the disclosures it has made or been required to make. This record should be available to the Commissioner and his inspectors to enable comparative scrutiny of the records kept by public authorities. Guidance on the maintenance of records by CSPs may be issued by or sought from IOCCO.

6.10. The records to be kept by a CSP, in respect of each notice or authorisation, should include:

A. the name of the public authority;

B. the URN of the notice or authorisation;

C. the date the notice was served upon the CSP or the authorisation disclosed to the CSP;

D. a description of any communications data required where no disclosure took place or could have taken place;

E. the date when the communications data was made available to the public authority or, where secure systems are provided by the CSP, the date when the acquisition and disclosure of communications data was undertaken; and

F. sufficient records to establish the origin and exact communications data that has been disclosed in the event of later challenge in court.

Errors

6.11. Proper application of RIPA and thorough procedures for operating its provisions, including the careful preparation and checking of applications, notices and authorisations, should reduce the scope for making errors whether by public authorities or by CSPs.

6.12. An error can only occur after a designated person:

64 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

- has granted an authorisation and the acquisition of data has been initiated; or
- has given notice and the notice has been served on a CSP in writing, electronically or orally.

6.13. Any failure by a public authority to apply correctly the process of acquiring or obtaining communications data set out in this code will increase the likelihood of an error occurring.

6.14. Where any error occurs in the grant of an authorisation, the giving of a notice or as a consequence of any authorised conduct, or any conduct undertaken to comply with a notice, a record should be kept.

6.15. Where an error results in communications data being acquired or disclosed wrongly, a report must be made to the Commissioner ('a reportable error'). Such errors can have very significant consequences on an affected individual's rights with details of their private communications being disclosed to a public authority and, in extreme circumstances, being wrongly detained or wrongly accused of a crime as a result of that error.

6.16. In cases where an error has occurred but is identified by the public authority or the CSP without data being acquired or disclosed wrongly, a record will be maintained by the public authority of such occurrences ('recordable error'). These records must be available for inspection by the Commissioner.

6.17. This section of the code cannot provide an exhaustive list of possible causes of reportable or recordable errors. Examples could include:

Reportable errors

- an authorisation or notice made for a purpose, or for a type of data, which the relevant public authority cannot call upon, or seek, under RIPA;
- human error, such as incorrect transposition of information from an application to an authorisation or notice where communications data is acquired or disclosed;
- disclosure of the wrong data by a CSP when complying with a notice; and
- acquisition of the wrong data by a public authority when engaging in conduct specified in an authorisation.

Recordable errors

- a notice has been given which is impossible for a CSP to comply with and the public authority attempts to impose the requirement;
- failure to review information already held, for example unnecessarily seeking the acquisition or disclosure of data already acquired or obtained for the same investigation or operation;
- the requirement to acquire or obtain the data is known to be no longer valid;
- failure to serve written notice (or where appropriate an authorisation) upon a CSP within one working day of urgent oral notice being given or an urgent oral authorisation granted; and

- human error, such as incorrect transposition of information from an application to an authorisation or notice where communications data is not acquired or disclosed.

6.18. Reporting and recording of errors will draw attention to those aspects of the process of acquisition and disclosure of communications data that require further improvement to eliminate errors and the risk of undue interference with any individual's rights.

6.19. When a reportable error has been made, the public authority which made the error, or established that the error had been made, must establish the facts and report the error to the authority's senior responsible officer and then to the IOCCO within no more than five working days of the error being discovered. All errors should be reported as they arise. If the report relates to an error made by a CSP, the public authority should also inform the CSP and IOCCO of the report in written or electronic form. This will enable the CSP and IOCCO to investigate the cause or causes of the reported error.

6.20. The report sent to the IOCCO by a public authority in relation to a reportable error must include details of the error, identified by the public authority's unique reference number of the relevant authorisation or notice, explain how the error occurred, indicate whether any unintended collateral intrusion has taken place and provide an indication of what steps have been, or will be, taken to ensure that a similar error does not recur. When a public authority reports an error made by a CSP, the report must include details of the error and indicate whether the CSP has been informed or not (in which case the public authority must explain why the CSP has not been informed of the report).

6.21. Where a CSP discloses communications data in error, it must report each error to the IOCCO within no more than five working days of the error being discovered. It is appropriate for a person holding a suitably senior position within a CSP to do so, identifying the error by reference to the public authority's unique reference number and providing an indication of what steps have been, or will be, taken to ensure that a similar error does not recur. Errors by service providers could include responding to a notice by disclosing incorrect data or by disclosing the required data to the wrong public authority.

6.22. In circumstances where a reportable error is deemed to be of a serious nature, the Commissioner may investigate the circumstances that led to the error and assess the impact of the interference on the affected individual's rights. The Commissioner may inform the affected individual, who may make a complaint to the Investigatory Powers Tribunal (see section 9).

6.23. The records kept by a public authority accounting for recordable errors must include details of the error, explain how the error occurred and provide an indication of what steps have been, or will be, taken to ensure that a similar error does not reoccur. The authority's senior responsible officer must undertake a regular review of the recording of such errors.

6.24. Where material which has no connection or relevance to any investigation or operation undertaken by the public authority receiving it is disclosed in error by a CSP, that material and any copy of it (including copies contained in or as attachments in electronic mail) should be destroyed as soon as the report to the Commissioner has been made.

...

66 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

Excess Data

6.26. Where authorised conduct by a public authority results in the acquisition of excess data, or its disclosure by a CSP in order to comply with the requirement of a notice, all the data acquired or disclosed should be retained by the public authority.

6.27. Where a public authority is bound by the CPIA and its code of practice, there will be a requirement to record and retain data which is relevant to a criminal investigation, even if that data was disclosed or acquired beyond the scope of a valid notice or authorisation. If a criminal investigation results in proceedings being instituted all material that may be relevant must be retained at least until the accused is acquitted or convicted or the prosecutor decides not to proceed.

6.28. If, having reviewed the excess data, it is intended to make use of the excess data in the course of the investigation or operation, an applicant must set out the reason(s) for needing to use that material in an addendum to the application upon which the authorisation or notice was originally granted or given. The designated person will then consider the reason(s) and review all the data and consider whether it is necessary and proportionate for the excess data to be used in the investigation or operation. As with all communications data acquired, the requirements of the DPA and its data protection principles must also be adhered to in relation to any excess data (see next section).

7 DATA PROTECTION SAFEGUARDS

7.1. Communications data acquired or obtained under the provisions of RIPA, and all copies, extracts and summaries of it, must be handled and stored securely. In addition, the requirements of the DPA and its data protection principles must be adhered to.

7.2. Communications data that is obtained directly as a consequence of the execution of an interception warrant must be treated in accordance with the safeguards which the Secretary of State has approved in accordance with section 15 of RIPA.

Disclosure of communications data and subject access rights

7.3. This section of the code provides guidance on the relationship between disclosure of communications data under RIPA and the provisions for subject access requests under the DPA, and the balance between CSPs' obligations to comply with a notice to disclose data and individuals' right of access under section 7 of the DPA to personal data held about them.

7.4. There is no provision in RIPA preventing CSPs from informing individuals about whom they have been required by notice to disclose communications data in response to a Subject Access Request made under section 7 of the DPA. However a CSP may exercise certain exemptions to the right of subject access under Part IV of the DPA.

7.5. Section 28 of the DPA provides that data are always exempt from section 7 where such an exemption is required for the purposes of safeguarding national security.

7.6. Section 29 of the DPA provides that personal data processed for the purposes of the prevention and detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of any tax or duty or other imposition of a similar nature are exempt from section 7 to the extent to which the application of the provisions for rights of data subjects would be likely to prejudice any of those matters.

7.7. The exemption to subject access rights possible under section 29 does not automatically apply to the disclosure of the existence of notices given under RIPA. In the event that a CSP receives a subject access request where the fact of a disclosure under RIPA might itself be disclosed, the CSP concerned must carefully consider whether in the particular case disclosure of the fact of the notice would be likely to prejudice the prevention or detection of crime.

7.8. Where a CSP is uncertain whether disclosure of the fact of a notice would be likely to prejudice an investigation or operation, it should approach the SPoC of the public authority which gave the notice – and do so in good time to respond to the subject access request. The SPoC can make enquiries within the public authority to determine whether disclosure of the fact of the notice would likely be prejudicial to the matters in section 29.

7.9. Where a CSP withholds a piece of information in reliance on the exemption in section 28 or 29 of the DPA, it is not obliged to inform an individual that any information has been withheld. It can simply leave out that piece of information and make no reference to it when responding to the individual who has made the subject access request.

7.10. CSPs should keep a record of the steps they have taken in determining whether disclosure of the fact of a notice would prejudice the apprehension or detection of offenders. This might be useful in the event of the data controller having to respond to enquiries made subsequently by the Information Commissioner, the courts and, in the event of prejudice, the police. Under section 42 of the DPA an individual may request that the Information Commissioner assesses whether a subject access request has been handled in compliance with the DPA.

Acquisition of communication data on behalf of overseas authorities

7.11. While the majority of public authorities which obtain communications data under RIPA have no need to disclose that data to any authority outside the United Kingdom, there can be occasions when it is necessary, appropriate and lawful to do so in matters of international co-operation.

7.12. There are two methods by which communications data, whether obtained under RIPA or not, can be acquired and disclosed to overseas public authorities:

- judicial co-operation; or
- non-judicial co-operation.

Neither method compels United Kingdom public authorities to disclose data to overseas authorities. Data can only be disclosed when a United Kingdom public authority is satisfied that it is in the public interest to do so and all relevant conditions imposed by domestic legislation have been fulfilled.

Judicial co-operation

7.13. A central authority in the United Kingdom may receive a request for mutual legal assistance (MLA) which includes a request for communications data from an overseas court exercising criminal jurisdiction, an overseas prosecuting authority, or any other overseas authority that appears to have a function of making requests for MLA. This MLA request must be made in connection with criminal proceedings or a criminal investigation being carried on outside the United Kingdom, and the request for communications data included must be capable of satisfying the requirements of Part I Chapter II of RIPA.

7.14. If such an MLA request is accepted by the central authority, it will be referred for consideration by the appropriate public authority in the UK. The application may then be considered and, if appropriate, executed by that public authority under section 22 of RIPA and in line with the guidance in this code of practice.

7.15. In order for a notice or authorisation to be granted, the United Kingdom public authority must be satisfied that the application meets the same criteria of necessity and proportionality as required for a domestic application.

Non-judicial co-operation

7.16. Public authorities in the United Kingdom can receive direct requests for assistance from their counterparts in other countries. These can include requests for the acquisition and disclosure of communications data for the purpose of preventing or detecting crime. On receipt of such a request, the United Kingdom public authority may consider seeking the acquisition or disclosure of the requested data under the provisions of Chapter II of Part I of RIPA.

7.17. The United Kingdom public authority must be satisfied that the request complies with United Kingdom obligations under human rights legislation. The necessity and proportionality of each case must be considered before the authority processes the authorisation or notice.

Disclosure of communications data to overseas authorities

7.18. Where a United Kingdom public authority is considering the acquisition of communications data on behalf of an overseas authority and transferring the data to that authority, it must consider whether the data will be adequately protected outside the United Kingdom and what safeguards may be needed to ensure that. Such safeguards might include attaching conditions to the processing, storage and destruction of the data.

7.19. If the proposed transfer of data is to an authority within the European Union, that authority will be bound by the European Data Protection Directive (95/46/EC) and its national data protection legislation. Any data disclosed will be protected there without need for additional safeguards.

7.20. If the proposed transfer is to an authority outside of the European Union and the European Economic Area (Iceland, Liechtenstein and Norway), then it must not be disclosed unless the overseas authority can ensure an adequate level of data protection. The European Commission has determined that certain countries, for example Switzerland, have laws providing an adequate level of protection where data can be transferred without need for further safeguards.

7.21. In all other circumstances, the United Kingdom public authority must decide in each case, before transferring any data overseas, whether the data will be adequately protected there. The Information Commissioner has published guidance on sending personal data outside the European Economic Area in compliance with the Eighth Data Protection Principle, and, if necessary, his office can provide guidance.

7.22. The DPA recognises that it will not always be possible to ensure adequate data protection in countries outside of the European Union and the European Economic Area, and there are exemptions to the principle, for example if the transfer of data is necessary for reasons of 'substantial public interest'. There may be circumstances when it is necessary, for example in the interests of national security, for communications data to be disclosed to a third party country, even though that country does not have adequate safeguards in place to protect the data. That is a

decision that can only be taken by the public authority holding the data on a case by case basis.

8 OVERSIGHT

8.1. RIPA provides for an Interception of Communications Commissioner (‘the Commissioner’) whose remit is to provide independent oversight of the exercise and performance of the powers and duties contained under Chapter II of Part I of RIPA. The Commissioner is supported by his inspectors who work from the Interception of Communications Commissioner’s Office (IOCCO).

8.2. This code does not cover the exercise of the Commissioner’s functions. It is the duty of any person who uses the powers conferred by Chapter II, or on whom duties are conferred, to comply with any request made by the Commissioner to provide any information he requires for the purposes of enabling him to discharge his functions.

8.3. Should the Commissioner establish that an individual has been adversely affected by any wilful or reckless failure by any person within a relevant public authority exercising or complying with the powers and duties under RIPA in relation to the acquisition or disclosure of communications data, he shall, subject to safeguarding national security, inform the affected individual of the existence of the Tribunal and its role. The Commissioner should disclose sufficient information to the affected individual to enable them to engage the Tribunal effectively.

8.4. Reports made by the Commissioner concerning the inspection of public authorities and their exercise and performance of powers under Chapter II may be made available by the Commissioner to the Home Office to promulgate good practice and help identify training requirements within public authorities and CSPs.

8.5. Subject to the approval of the Commissioner, public authorities may publish their inspection reports, in full or in summary, to demonstrate both the oversight to which they are subject and their compliance with Chapter II of RIPA and this code. Approval should be sought on a case by case basis at least ten working days prior to intended publication, stating whether the report is to be published in full, and, if not, stating which parts are to be published or how it is to be summarised.”

3. *News Group and Others v. The Commissioner of Police of the Metropolis IPT/14/176/H, 17 December 2015*

118. These proceedings were brought before the IPT by three journalists and their employer. They challenged four authorisations issued under section 22 of RIPA with the purpose of enabling police to obtain communications data which might reveal sources of information obtained by the journalists. They argued, *inter alia*, that the section 22 regime (at the time supplemented by the 2007 Code of Practice) breached their rights under Article 10 of the Convention as it did not adequately safeguard the confidentiality of journalists’ sources. The IPT agreed that the regime in place at the time did not contain effective safeguards to protect Article 10 rights in a case in which the authorisation had the purpose of obtaining disclosure of the identity of a journalist’s source. It held:

“107. In the absence of a requirement for prior scrutiny by a court, particular regard must be paid to the adequacy of the other safeguards prescribed by the law. The designated person is not independent of the police force, although in practice, properly

complying with the requirements of s 22, he will make an independent judgement, as he did in this case. In general the requirement for a decision on necessity and proportionality to be taken by a senior officer who is not involved in the investigation does provide a measure of protection as to process, but the role of the designated person cannot be equated to that of an independent and impartial judge or tribunal.

108. Subsequent oversight by the Commissioner, or, in the event of a complaint, by this Tribunal, cannot after the event prevent the disclosure of a journalist's source. This is in contrast to criminal investigations where a judge at a criminal trial may be able to exclude evidence which has been improperly or unfairly obtained by an authorisation made under s 22. Where an authorisation is made which discloses a journalist's source that disclosure cannot subsequently be reversed, nor the effect of such disclosure mitigated. Nor was there any requirement in the 2007 Code for any use of s 22 powers for the purpose of obtaining disclosure of a journalist's source to be notified to the Commissioner, so in such cases this use of the power might not be subject to any effective review. Furthermore none of the Complainants had any reason to suspect that their data had been accessed until the closing report on Operation Alice was published in September 2014. If the Respondent had not disclosed that information – and it is to his credit that he did – then the Complainants would never have been in a position to bring these proceedings.

109. So in a case involving the disclosure of a journalist's source the safeguards provided for under s 22 and the 2007 Code were limited to requiring a decision as to necessity and proportionality to be made by a senior police officer, who was not directly involved in the investigation and who had a general working knowledge of human rights law. The 2007 Code imposed no substantive or procedural requirement specific to cases affecting the freedom of the press. There was no requirement that an authorisation should only be granted where the need for disclosure was convincingly established, nor that there should be very careful scrutiny balancing the public interest in investigating crime against the protection of the confidentiality of journalistic sources. The effect of s 22 and the 2007 Code was that the designated person was to make his decision on authorisation on the basis of the same general tests of necessity and proportionality which would be applied to an application in any criminal investigation.”

119. The IPT could not award any remedy in respect of the failure to provide adequate safeguards to protect Article 10 rights, as this did not in itself render the authorisations unlawful. However, it also found that one of the authorisations was unlawful, as it had been neither proportionate nor necessary. In considering the appropriate remedy, it acknowledged that it had the power to award compensation, but declined to do so since it did not consider it necessary to afford just satisfaction.

120. In March 2015 the 2007 Code of Practice was replaced by a new code. Paragraph 3.78 of that new ACD Code provides that in the specific case of an application for communications data, which is made in order to identify a journalist's source, those law enforcement agencies with powers under the Police and Criminal Evidence Act 1984 (PACE) must use the procedures of PACE to apply to a court for a production order to obtain this data.

4. *The Police and Criminal Evidence Act 1984*

121. Schedule 1 of PACE governs the procedure for applying to court for a production order. It provides, as relevant:

“1. If on an application made by a constable a judge is satisfied that one or other of the sets of access conditions is fulfilled, he may make an order under paragraph 4 below.

...

4. An order under this paragraph is an order that the person who appears to the judge to be in possession of the material to which the application relates shall—

- (a) produce it to a constable for him to take away; or
- (b) give a constable access to it,

not later than the end of the period of seven days from the date of the order or the end of such longer period as the order may specify.

...

7. An application for an order under paragraph 4 above that relates to material that consists of or includes journalistic material shall be made *inter partes*.”

122. Section 78 of PACE permits a court to refuse to allow evidence on which the prosecution proposes to rely to be given if it appears to the court that, having regard to all the circumstances, including the circumstances in which the evidence was obtained, the admission of the evidence would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it.

D. IPT practice and procedure

1. *RIPA*

123. The IPT was established under section 65(1) of RIPA to hear allegations by citizens of wrongful interference with their communications as a result of conduct covered by that Act. Members must hold or have held high judicial office or be a qualified lawyer of at least ten years’ standing.

124. Section 65(2) provides that the IPT is the only appropriate forum in relation to proceedings against any of the intelligence services for acts allegedly incompatible with Convention rights, and complaints by persons who allege to have been subject to the investigatory powers of RIPA. It has jurisdiction to investigate any complaint that a person’s communications have been intercepted and, where interception has occurred, to examine the authority for such interception.

125. According to sections 67(2) and 67(3)(c), the IPT is to apply the principles applicable by a court on an application for judicial review. It does not, however, have power to make a Declaration of Incompatibility if it finds primary legislation to be incompatible with the European Convention

on Human Rights as it is not a “court” for the purposes of section 4 of the Human Rights Act 1998.

126. Under section 67(8), there is no appeal from a decision of the IPT “except to such extent as the Secretary of State may by order otherwise provide”. No such order has been made by the Secretary of State. Furthermore, in *R(Privacy International) v. Investigatory Powers Tribunal* [2017] EWCA Civ 1868 the Court of Appeal recently confirmed that section 67(8) also had the effect of preventing a judicial review claim from being brought against a decision of the IPT. As a consequence, the IPT is a court of last resort for the purposes of the obligation to request a preliminary ruling under Article 267 of the Treaty on the Functioning of the European Union (see paragraph 236 below).

127. Section 68(6) and (7) requires those involved in the authorisation and execution of an interception warrant to disclose or provide to the IPT all documents and information it may require.

128. Section 68(4) provides that where the IPT determines any complaint it has the power to award compensation and to make such other orders as it thinks fit, including orders quashing or cancelling any warrant and orders requiring the destruction of any records obtained thereunder (section 67(7)). In the event that a claim before the IPT is successful, the IPT is generally required to make a report to the Prime Minister (section 68(5)).

129. Section 68(1) entitles the IPT to determine its own procedure, although section 69(1) provides that the Secretary of State may also make procedural rules.

2. *The Investigatory Powers Tribunal Rules 2000 (“the Rules”)*

130. The Rules were adopted by the Secretary of State to govern various aspects of the procedure before the IPT.

131. Although the IPT is under no duty to hold oral hearings, pursuant to Rule 9 it may hold, at any stage of consideration, oral hearings at which the complainant may make representations, give evidence and call witnesses. It may also hold separate oral hearings which the person whose conduct is the subject of the complaint, the public authority against which the proceedings are brought, or any other person involved in the authorisation or execution of an interception warrant may be required to attend. Rule 9 provides that the IPT’s proceedings, including any oral hearings, are to be conducted in private.

132. Rule 11 allows the IPT to receive evidence in any form, even where it would not be admissible in a court of law. It may require a witness to give evidence on oath, but no person can be compelled to give evidence at an oral hearing under Rule 9(3).

133. Rule 13 provides guidance on notification to the complainant of the IPT’s findings:

“(1) In addition to any statement under section 68(4) of the Act, the Tribunal shall provide information to the complainant in accordance with this rule.

(2) Where they make a determination in favour of the complainant, the Tribunal shall provide him with a summary of that determination including any findings of fact.

...

(4) The duty to provide information under this rule is in all cases subject to the general duty imposed on the Tribunal by rule 6(1).

(5) No information may be provided under this rule whose disclosure would be restricted under rule 6(2) unless the person whose consent would be needed for disclosure under that rule has been given the opportunity to make representations to the Tribunal.”

134. Rule 6 requires the IPT to carry out its functions in such a way as to ensure that information is not disclosed that is contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime, the economic well-being of the United Kingdom or the continued discharge of the functions of any of the intelligence services. Pursuant to Rule 6, in principle, the IPT is not permitted to disclose: the fact that it has held an oral hearing under Rule 9(4); any information disclosed to it in the course of that hearing or the identity of any witness at that hearing; any information otherwise disclosed to it by any person involved in the authorisation or execution of interception warrants, or any information provided by a Commissioner; and the fact that any information has been disclosed or provided. However, the IPT may disclose such information with the consent of the person required to attend the hearing, the person who disclosed the information, the Commissioner, or the person whose consent was required for disclosure of the information, as the case may be. The IPT may also disclose such information as part of the information provided to the complainant under Rule 13(2), subject to the restrictions contained in Rule 13(4) and (5).

135. In *R(A) v. Director of Establishments of the Security Service* [2009] EWCA Civ 24 Lord Justice Laws observed that the IPT was “a judicial body of like standing and authority to the High Court”. More recently, in *R(Privacy International) v. Investigatory Powers Tribunal* (cited above) Lord Justice Sales noted that “[t]he quality of the membership of the IPT in terms of judicial expertise and independence is very high”.

3. IPT ruling on preliminary issues of law

136. On 23 January 2003, in a case involving a complaint by British-Irish Rights Watch, the IPT gave a ruling on preliminary issues of law, in which it considered whether a number of aspects of its procedure were within the powers conferred on the Secretary of State and Convention compliant. The IPT sat, for the first time, in public.

137. Specifically on the applicability of Article 6 § 1 to the proceedings before it, the IPT found:

“85. The conclusion of the Tribunal is that Article 6 applies to a person’s claims under section 65(2)(a) and to his complaints under section 65(2)(b) of RIPA, as each of them involves ‘the determination of his civil rights’ by the Tribunal within the meaning of Article 6(1).”

138. The IPT considered that Rule 9 made it clear that oral hearings could be held at its discretion. If a hearing was held, it had to be held in accordance with Rule 9. The absence from the Rules of an absolute right to either an *inter partes* oral hearing, or, failing that, to a separate oral hearing in every case was within the rule-making power in section 69(1) of RIPA and was compatible with the Convention rights under Article 6, 8 and 10. The IPT explained that oral hearings involving evidence or a consideration of the substantive merits of a claim or complaint ran the risk of breaching the “neither confirm nor deny” policy or other aspects of national security and the public interest. It was therefore necessary to provide safeguards against that and the conferring of a discretion to decide when there should be oral hearings and what form they should take was a proportionate response to the need for safeguards.

139. The IPT found the language in Rule 9(6), which stipulates that oral hearings must be held in private, to be clear and unqualified; it therefore had no discretion in the matter. It concluded that the width and blanket nature of the rule went beyond what was authorised by section 69 of RIPA and, as a consequence, it found Rule 9(6) to be *ultra vires* section 69 and not binding on it.

140. The IPT also considered the requirements in Rule 6 for the taking of evidence and disclosure. It concluded that these departures from the adversarial model were within the power conferred on the Secretary of State and compatible with Convention rights in Articles 8 and 10, taking account of the exceptions for the public interest and national security in Articles 8(2) and 10(2), and in particular the effective operation of the legitimate policy of “neither confirm nor deny” in relation to the use of investigatory powers. It noted that disclosure of information was not an absolute right where there were competing interests, such as national security considerations.

141. Finally, as regards the absence of reasons following a negative decision, the IPT concluded that section 68(4) and Rule 13 were valid and binding and that the distinction between information given to the successful complainants and that given to unsuccessful complainants (where the “neither confirm nor deny” policy had to be preserved) was necessary and justifiable.

4. *Counsel to the Tribunal*

142. The IPT may appoint Counsel to the Tribunal to make submissions on behalf of applicants in hearings at which they cannot be represented. In the *Liberty* case, Counsel to the Tribunal described his role as follows:

“Counsel to the Tribunal performs a different function [from special advocates in closed proceedings conducted before certain tribunals], akin to that of *amicus curiae*. His or her function is to assist the Tribunal in whatever way the Tribunal directs. Sometimes (e.g. in relation to issues on which all parties are represented), the Tribunal will not specify from what perspective submissions are to be made. In these circumstances, counsel will make submissions according to his or her own analysis of the relevant legal or factual issues, seeking to give particular emphasis to points not fully developed by the parties. At other times (in particular where one or more interests are not represented), the Tribunal may invite its counsel to make submissions from a particular perspective (normally the perspective of the party or parties whose interests are not otherwise represented).”

143. This description was accepted and endorsed by the IPT.

E. Oversight

144. Part IV of RIPA provided for the appointment by the Prime Minister of an Interception of Communications Commissioner and an Intelligence Services Commissioner charged with supervising the activities of the intelligence services.

145. The Interception of Communications Commissioner was responsible for keeping under review the interception of communications and the acquisition and disclosure of communications data by intelligence agencies, police forces and other public authorities. He reported to the Prime Minister on a half-yearly basis with respect to the carrying out of his functions. This report was a public document (subject to the non-disclosure of confidential annexes) which was laid before Parliament. In undertaking his review of surveillance practices, the Commissioner and his inspectors had access to all relevant documents, including closed materials, and all those involved in interception activities had a duty to disclose to him any material he required. The obligation on intercepting agencies to keep records ensured that the Commissioner had effective access to details of surveillance activities undertaken.

146. The Intelligence Services Commissioner also provided independent external oversight of the use of the intrusive powers of the intelligence services and parts of the Ministry of Defence. He also submitted annual reports to the Prime Minister, which were laid before Parliament.

147. However, these provisions, insofar as they relate to England, Scotland and Wales, were repealed by the Investigatory Powers Act 2016 (see paragraphs 195-201 below) and in September 2017 the Investigatory Powers Commissioner’s Office (“IPCO”) took over responsibility for the

oversight of investigatory powers. The IPCO consists of around fifteen Judicial Commissioners, current and recently retired High Court, Court of Appeal and Supreme Court Judges; a Technical Advisory Panel made up of scientific experts; and almost fifty official staff, including inspectors, lawyers and communications experts. The more intrusive powers such as interception, equipment interference and the use of surveillance in sensitive environments will be subject to the prior approval of a Judicial Commissioner once the provisions of the 2016 Act have entered into force. Use of these and other surveillance powers, including the acquisition of communications data and the use of covert human intelligence sources, are also overseen by a programme of retrospective inspection and audit by Judicial Commissioners and IPCO's inspectors.

F. Reviews of interception operations by the intelligence service

1. Intelligence and Security Committee of Parliament: July 2013 Statement on GCHQ's alleged interception of communications under the US PRISM programme

148. The Intelligence and Security Committee of Parliament ("the ISC") was originally established by the Intelligence Services Act 1994 to examine the policy, administration and expenditure of MI5, MI6, and GCHQ. Since the introduction of the Justice and Security Act 2013, however, the ISC was expressly given the status of a Committee of Parliament; was provided with greater powers; and its remit was increased to include *inter alia* oversight of operational activity and the wider intelligence and security activities of Government. Pursuant to sections 1-4 of the Justice and Security Act 2013, it consists of nine members drawn from both Houses of Parliament, and, in the exercise of their functions, those members are routinely given access to highly classified material in carrying out their duties.

149. Following the Edward Snowden revelations, the ISC conducted an investigation into GCHQ's access to the content of communications intercepted under the US PRISM programme, the legal framework governing access, and the arrangements GCHQ had with its overseas counterpart for sharing information. In the course of the investigation, the ISC took detailed evidence from GCHQ and discussed the programme with the NSA.

150. The ISC concluded that allegations that GCHQ had circumvented United Kingdom law by using the NSA PRISM programme to access the content of private communications were unfounded as GCHQ had complied with its statutory duties contained in the ISA. It further found that in each case where GCHQ sought information from the United States, a warrant for interception, signed by a Government Minister, had already been in place. However, it found it necessary to further consider whether the current

statutory framework governing access to private communications remained accurate.

2. Privacy and security: a modern and transparent legal framework

151. Following its statement in July 2013, the ISC conducted a more in-depth inquiry into the full range of the intelligence services' capabilities. Its report, which contained an unprecedented amount of information about the intelligence services' intrusive capabilities, was published on 12 March 2015 (see paragraphs 11-13 above).

152. The ISC was satisfied that the United Kingdom's intelligence and security services did not seek to circumvent the law, including the requirements of the Human Rights Act 1998, which governs everything that they do. However, it considered that as the legal framework had developed piecemeal, it was unnecessarily complicated. The ISC therefore had serious concerns about the resulting lack of transparency, which was not in the public interest. Consequently, its key recommendation was that the current legal framework be replaced by a new Act of Parliament which should clearly set out the intrusive powers available to the intelligence services, the purposes for which they may use them, and the authorisation required before they may do so.

153. With regard to GCHQ's bulk interception capability, the inquiry showed that the intelligence services did not have the legal authority, the resources, the technical capability, or the desire to intercept every communication of British citizens, or of the Internet as a whole: thus, GCHQ were not reading the emails of everyone in the United Kingdom. On the contrary, GCHQ's bulk interception systems operated on a very small percentage of the bearers that made up the Internet and the ISC was satisfied that GCHQ applied levels of filtering and selection such that only a certain amount of the material on those bearers was collected. Further targeted searches ensured that only those items believed to be of the highest intelligence value were ever presented for analysts to examine, and therefore only a tiny fraction of those collected were ever seen by human eyes.

154. In respect of Internet communications, the ISC considered that the current system of 'internal' and 'external' communications was confusing and lacked transparency and it therefore suggested that the Government publish an explanation of which Internet communications fall under which category, including a clear and comprehensive list of communications.

155. Nevertheless, the inquiry had established that bulk interception could not be used to target the communications of an individual in the United Kingdom without a specific authorisation naming that individual, signed by a Secretary of State.

156. With regard to section 8(4) warrants, the ISC observed that the warrant itself was very brief. It further noted that insofar as the

accompanying certificate set out the categories of communications which might be examined, those categories were expressed in very general terms (for example, “material providing intelligence on terrorism (as defined by the Terrorism Act 2000 (as amended)), including, but not limited to, terrorist organisations, terrorists, active sympathisers, attack planning, fund-raising”). Given that the certificate was so generic, the ISC questioned whether it needed to be secret or whether, in the interests of transparency, it could be published.

157. Although the section 8(4) certificate set out the general categories of information which might be examined, the ISC observed that in practice, it was the selection of the bearers, the application of simple selectors and initial search criteria, and then complex searches which determined what communications were examined. The ISC had therefore sought assurances that these were subject to scrutiny and review by Ministers and/or the Commissioners. However, the evidence before the ISC indicated that neither Ministers nor the Commissioners had any significant visibility of these issues. The ISC therefore recommended that the Interception of Communications Commissioner should be given statutory responsibility to review the various selection criteria used in bulk interception to ensure that they followed directly from the Certificate and valid national security requirements.

158. The ISC noted that communications data was central to most intelligence services’ investigations: it could be analysed to find patterns that reflected particular online behaviours associated with activities such as attack planning, and to establish links, to help focus on individuals who might pose a threat, to ensure that interception was properly targeted, and to illuminate networks and associations relatively quickly. It was particularly useful in the early stages of an investigation, when the intelligence services had to be able to determine whether those associating with a target were connected to the plot (and therefore required further investigation) or were innocent bystanders. According to the Secretary of State for the Home Department, it had “played a significant role in every Security Service counter-terrorism operation over the last decade”. Nevertheless, the ISC expressed concern about the definition of “communications data”. While it accepted that there was a category of communications data which was less intrusive than content, and therefore did not require the same degree of protection, it considered that there now existed certain categories of communications data which had the potential to reveal more intrusive details about a person’s private life and, therefore, required greater safeguards.

159. Finally, with regard to the IPT, it expressly recognised the importance of a domestic right of appeal.

3. *“A Question of Trust”: Report of the Investigatory Powers Review by the Independent Reviewer of Terrorism Legislation (“the Anderson Report”)*

160. The Independent Reviewer of Terrorism Legislation, a role that has existed since the late 1970s, is an independent person, appointed by the Home Secretary and by the Treasury for a renewable three-year term and tasked with reporting to the Home Secretary and to Parliament on the operation of counter-terrorism law in the United Kingdom. These reports are then laid before Parliament, to inform the public and political debate. The Independent Reviewer’s role is to inform the public and political debate on anti-terrorism law in the United Kingdom. The uniqueness of the role lies in its complete independence from government, coupled with access based on a very high degree of clearance to secret and sensitive national security information and personnel.

161. The purpose of the Anderson Report, published in June 2015 and identified by reference to the then Independent Reviewer of Terrorism Legislation, was to inform the public and political debate on the threats to the United Kingdom, the capabilities required to combat those threats, the safeguards in place to protect privacy, the challenges of changing technology, issues relating to transparency and oversight, and the case for new or amended legislation. In conducting the review the Independent Reviewer had unrestricted access, at the highest level of security clearance, to the responsible Government departments and public authorities. He also engaged with service providers, independent technical experts, non-governmental organisations, academics, lawyers, judges and regulators.

162. The Independent Reviewer noted that the statutory framework governing investigatory powers had developed in a piecemeal fashion, with the consequence that there were “few [laws] more impenetrable than RIPA and its satellites”.

163. With regard to the importance of communications data, he observed that it enabled the intelligence services to build a picture of a subject of interest’s activities and was extremely important in providing information about criminal and terrorist activity. It identified targets for further work and also helped to determine if someone was completely innocent. Of central importance was the ability to use communications data (subject to necessity and proportionality) for:

- (a) linking an individual to an account or action (for example, visiting a website, sending an email) through IP resolution;
- (b) establishing a person’s whereabouts, traditionally via cell site or GPRS data;
- (c) establishing how suspects or victims are communicating (that is, via which applications or services);

80 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

(d) observing online criminality (for example, which websites are being visited for the purposes of terrorism, child sexual exploitation or purchases of firearms or illegal drugs); and

(e) exploiting data (for example, to identify where, when and with whom or what someone was communicating, how malware or a denial of service attack was delivered, and to corroborate other evidence).

164. Moreover, analysis of communications data could be performed speedily, making it extremely useful in fast-moving operations, and use of communications data could build a case for using a more intrusive measure, or deliver the information that would make other measures unnecessary.

165. His proposals for reform can be summarised as follows:

(a) A comprehensive and comprehensible new law should be drafted, replacing “the multitude of current powers” and providing clear limits and safeguards on any intrusive power it may be necessary for public authorities to use;

(b) The definitions of “content” and “communications data” should be reviewed, clarified and brought up-to-date;

(c) The capability of the security and intelligence agencies to practice bulk collection of intercepted material and associated communications data should be retained, but only subject to strict additional safeguards including the authorisation of all warrants by a Judicial Commissioner at a new Independent Surveillance and Intelligence Commission (“ISIC”);

(d) The purposes for which material or data was sought should be spelled out in the accompanying certificate by reference to specific operations or mission purposes (for example, “attack planning by ISIL in Iraq/Syria against the UK”);

(e) There should be a new form of bulk warrant limited to the acquisition of communications data which could be a proportionate option in certain cases;

(f) Regarding the authorisation for the acquisition of communications data, designated persons should be required by statute to be independent from the operations and investigations in relation to which the authorisation is sought;

(g) Novel or contentious requests for communications data, or requests for the purpose of determining matters that are privileged or confidential, should be referred to the ISIC for determination by a Judicial Commissioner;

(h) The ISIC should take over intelligence oversight functions and should be public-facing, transparent and accessible to the media; and

(i) The IPT should have the capacity to make declarations of incompatibility and its rulings should be subject to appeals on points of law.

4. A Democratic Licence to Operate: Report of the Independent Surveillance Review (“ISR”)

166. The ISR was undertaken by the Royal United Services Institute, an independent think-tank, at the request of the then deputy Prime Minister, partly in response to the revelations by Edward Snowden. Its terms of reference were to look at the legality of United Kingdom surveillance programmes and the effectiveness of the regimes that govern them, and to suggest reforms which might be necessary to protect both individual privacy and the necessary capabilities of the police and security and intelligence services.

167. Despite the revelations by Edward Snowden, having completed its review the ISR found no evidence that the British Government was knowingly acting illegally in intercepting private communications, or that the ability to collect data in bulk was being used by the Government to provide it with a perpetual window into the private lives of British citizens. On the other hand, it found evidence that the present legal framework authorising the interception of communications was unclear, had not kept pace with developments in communications’ technology, and did not serve either the Government or members of the public satisfactorily. It therefore concluded that a new, comprehensive and clearer legal framework was required.

168. In particular, it supported the view set out in both the ISC and Anderson reports that while the current surveillance powers were needed, both a new legislative framework and oversight regime were required. It further considered that the definitions of “content” and “communications data” should be reviewed as part of the drafting of the new legislation so that they could be clearly delineated in law.

169. With regard to communications data, the report noted that greater volumes were available on an individual relative to content, since every piece of content was surrounded by multiple pieces of communications data. Furthermore, aggregating data sets could create an extremely accurate picture of an individual’s life since, given enough raw data, algorithms and powerful computers could generate a substantial picture of the individual and his or her patterns of behaviour without ever accessing content. In addition, the use of increasingly sophisticated encryption methods had made content increasingly difficult to access.

170. It further considered that the capability of the security and intelligence services to collect and analyse intercepted material in bulk should be maintained, but with the stronger safeguards recommended in the Anderson Report. In particular, it agreed that warrants for bulk interception should include much more detail than is currently the case and should be the subject of a judicial authorisation process, save for when there is an urgent requirement.

171. In addition, it agreed with both the ISC and the Anderson report that there should be different types of warrant for the interception and acquisition of communications and related data. It was proposed that warrants for a purpose relating to the detection or prevention of serious and authorised crime should always be authorised by a Judicial Commissioner, while warrants for purposes relating to national security should be authorised by the Secretary of State subject to judicial review by a Judicial Commissioner.

172. With regard to the IPT, the ISR recommended open public hearings, except where it was satisfied private or closed hearings were necessary in the interests of justice or other identifiable public interest. Furthermore, it should have the ability to test secret evidence put before it, possibly through the appointment of Special Counsel. Finally, it agreed with the ISC and Anderson reports that a domestic right of appeal was important and should be considered in future legislation.

5. Report of the Bulk Powers Review

173. The bulk powers review was set up in May 2016 to evaluate the operational case for the four bulk powers contained in what was then the Investigatory Powers Bill (now the Investigatory Powers Act 2016: see paragraphs 195-201 below). Those powers related to bulk interception and the bulk acquisition of communications data, bulk equipment interference and the acquisition of bulk personal datasets.

174. The review was again carried out by the Independent Reviewer of Terrorism Legislation. To conduct the review he recruited three team members, all of whom had the necessary security clearance to access very highly classified material, including a person with the necessary technical background to understand the systems and techniques used by GCHQ, and the uses to which they could be put; an investigator with experience as a user of secret intelligence, including intelligence generated by GCHQ; and senior independent counsel with the skills and experience to challenge forensically the evidence and the case studies presented by the security and intelligence services.

175. In conducting their review, the team had significant and detailed contact with the intelligence services at all levels of seniority as well as the relevant oversight bodies (including the IPT and Counsel to the Tribunal in the relevant cases), NGOs and independent technical experts.

176. Although the review was of the Investigatory Powers Bill, a number of its findings in respect of bulk interception are relevant to the case at hand. In particular, having examined a great deal of closed material, the review concluded that it was an essential capability: first, because terrorists, criminal and hostile foreign intelligence services had become increasingly sophisticated at evading detection by traditional means; and secondly, because the nature of the global Internet meant that the route a particular

communication would travel had become hugely unpredictable. The review team looked at alternatives to bulk interception (including targeted interception, the use of human sources and commercial cyber-defence products) but concluded that no alternative or combination of alternatives would be sufficient to substitute for the bulk interception power as a method of obtaining the necessary intelligence.

6. Attacks in London and Manchester March-June 2017: Independent Assessment of MI5 and Police Internal Reviews

177. Following a series of four terrorist attacks in the short period between March and June 2017, in the course of which some 36 innocent people were killed and almost 200 more were injured, the Home Secretary asked the recently retired Independent Reviewer of Terrorism Legislation, David Anderson Q.C. to assess the classified internal reviews of the police and intelligence services involved. In placing the attacks in context, the Report made the following observations:

“1.2 The attacks under review were the most deadly terrorist attacks on British soil since the 7/7 London tube and bus bombings of July 2005. All four were shocking for their savagery and callousness. The impact of the first three attacks was increased by the fact that they came at the end of a long period in which Islamist terrorism had taken multiple lives in neighbouring countries such as France, Belgium and Germany but had not enjoyed equivalent success in Britain.

1.3 The plots were part of an increasingly familiar pattern of Islamist and (to a lesser extent) anti-Muslim terrorist attacks in western countries, including in particular northern Europe. The following points provide context, and an indication that lessons learned from these incidents are likely to be transferrable.

1.4 First, the *threat level* in the UK from so-called “international terrorism” (in practice, Islamist terrorism whether generated at home or abroad) has been assessed by the Joint Terrorism Analysis Centre (JTAC) as SEVERE since August 2014, indicating that Islamist terrorist attacks in the UK are “highly likely”. Commentators with access to the relevant intelligence have always been clear that this assessment is realistic. They have pointed also to the smaller but still deadly threat from extreme right wing (XRW) terrorism, exemplified by the murder of Jo Cox MP in June 2016 and by the proscription of the neo-Nazi group National Action in December 2016.

1.5 Secondly, the *growing scale* of the threat from Islamist terrorism is striking. The Director General of MI5, Andrew Parker, spoke in October 2017 of “a dramatic upshift in the threat this year” to “the highest tempo I’ve seen in my 34 year career”. Though deaths from Islamist terrorism occur overwhelmingly in Africa, the Middle East and South Asia, the threat has grown recently across the western world, and has been described as “especially diffuse and diverse in the UK”. It remains to be seen how this trend will be affected, for good or ill, by the physical collapse of the so-called Islamic State in Syria and Iraq.

1.6 Thirdly, the profiles of the *attackers* ... display many familiar features. Comparing the five perpetrators of the Westminster, Manchester and London Bridge attacks with those responsible for the 269 Islamist-related terrorist offences in the UK between 1998-2015, as analysed by Hannah Stuart (“the total”):

84 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

- (a) All were *male*, like 93% of the total.
- (b) Three were *British* (Masood, Abedi, Butt), like 72% of the total.
- (c) One was a *convert to Islam* (Masood), like 16% of the total.
- (d) Three *resided* in London (43% of the total) and one in North West England (10% of the total).
- (e) Three (Masood, and to a more limited extent Abedi and Butt) were *known to the police*, like 38% of the total.
- (f) The same three were *known to MI5*, like 48% of the total.
- (g) At least one (Butt) had direct links to a *proscribed terrorist organisation*, as had 44% of the total. His links, in common with 56% of the total who had links with such organisations, were with *Al-Muhajiroun* (ALM).

In view of their possible pending trials I say nothing of Hashem Abedi, currently detained in Libya in connection with the Manchester attack, or of the Finsbury Park attacker Darren Osborne who (like Khalid Masood at Westminster) is not alleged to have had accomplices.

1.7 Fourthly, though the *targets* of the first three attacks did not extend to the whole of the current range, they had strong similarities to the targets of other recent western attacks: political centres (e.g. Oslo 2011, Ottawa 2014, Brussels 2016); concert-goers, revellers and crowds (e.g. Orlando 2016, Paris 2016, Barcelona 2017); and police officers (e.g. Melbourne 2014, Berlin 2015, Charleroi 2016). There are precedents also for attacks on observant Muslims which have crossed the boundary from hate crime to terrorism, including the killing of Mohammed Saleem in the West Midlands in 2013.

1.8 Fifthly, the *modus operandi* (MO) of terrorist attacks has diversified and simplified over the years, as Daesh has employed its formidable propaganda effort to inspire rather than to direct acts of terrorism in the west. The attacks under review were typical in style for their time and place:

- (a) Unlike the large, directed Islamist plots characteristic of the last decade, all four attacks were committed by *lone actors* or *small groups*, with little evidence of detailed planning or precise targeting.
- (b) Strong gun controls in the UK mean that *bladed weapons* are more commonly used than firearms in gang-related and terrorist crime.
- (c) Since a truck killed 86 innocent people in Nice (July 2016), *vehicles* – which featured in three of the four attacks under review – have been increasingly used as weapons.
- (d) The *combination* of a vehicle and bladed weapons, seen at Westminster and London Bridge, had previously been used to kill the soldier Lee Rigby (Woolwich, 2013).
- (e) *Explosives*, used in Manchester, were the most popular weapon for Islamist terrorists targeting Europe between 2014 and 2017. The explosive TATP has proved to be capable of manufacture (aided by on-line purchases and assembly instructions) more easily than was once assumed.”

7. *Annual Report of the Interception of Communications Commissioner for 2016*

(a) **Section 8(4) warrants**

178. The Commissioner observed that when conducting interception under a section 8(4) warrant, an intercepting agency had to use its knowledge of the way in which international communications were routed, combined with regular surveys of relevant communications links, to identify those individual communications bearers that were most likely to contain external communications that would meet the descriptions of material certified by the Secretary of State under section 8(4). It also had to conduct the interception in ways that limited the collection of non-external communications to the minimum level compatible with the objective of intercepting the wanted external communications.

179. He further observed that prior to analysts being able to read, look at or listen to material, they had to provide a justification, which included why access to the material was required, consistent with, and pursuant to section 16 and the applicable certificate, and why such access was proportionate. Inspections and audits showed that although the selection procedure was carefully and conscientiously undertaken, it relied on the professional judgment of analysts, their training and management oversight.

180. According to the report, 3007 interception warrants were issued in 2016 and five applications were refused by a Secretary of State. In the view of the Commissioner, these figures did not capture the critical quality assurance function initially carried out by the staff and lawyers within the intercepting agency or the warrant-granting department (the warrant-granting departments were a source of independent advice to the Secretary of State and performed pre-authorisation scrutiny of warrant applications and renewals to ensure that they were (and remained) necessary and proportionate). Based on his inspections, he was confident that the low number of rejections reflected the careful consideration given to the use of these powers.

181. A typical inspection of an interception agency included the following:

- 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 were sufficient for the purposes of Chapter 1 of Part 1 of RIPA and that all relevant records had been kept;
- the 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;

86 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

- interviews with case officers, analysts and/or linguists from selected investigations or operations to assess whether the interception and the justifications for acquiring all of the material were proportionate;
 - the examination of any urgent oral approvals to check that the process was justified and used appropriately;
 - a review of those cases where communications subject to legal privilege or otherwise confidential information had been intercepted and retained, and any cases where a lawyer was the subject of an investigation;
 - a review of the adequacy of the safeguards and arrangements under sections 15 and 16 of RIPA;
 - an investigation of the procedures in place for the retention, storage and destruction of intercepted material and related communications data; and
 - a review of the errors reported, including checking that the measures put in place to prevent recurrence were sufficient.
182. After each inspection, inspectors produced a report, including:
- an assessment of how far the recommendations from the previous inspection had been achieved;
 - a summary of the number and type of interception documents selected for inspection, including a detailed list of those warrants;
 - detailed comments on all warrants selected for further examination and discussion during the inspection;
 - an assessment of the errors reported to the Commissioner's office during the inspection period;
 - an account of the examination of the retention, storage and destruction procedures;
 - an account of other policy or operational issues which the agency or warrant-granting departments raised during the inspection;
 - an assessment of how any material subject to legal professional privilege (or otherwise confidential material) has been handled;
 - a number of recommendations aimed at improving compliance and performance.

183. During 2016, the Commissioner's office inspected all nine interception agencies once and the four main warrant-granting departments twice. This, together with extra visits to GCHQ, made a total of twenty-two inspection visits. In addition, he and his inspectors arranged other *ad hoc* visits to agencies.

184. Inspection of the systems in place for applying for and authorising interception warrants usually involved a three-stage process. First, to achieve a representative sample of warrants, inspectors selected them across different crime types and national security threats. In addition, inspectors

focussed on those of particular interest or sensitivity (such as those which gave rise to an unusual degree of collateral intrusion, those which have been extant for a considerable period, those which were approved orally, those which resulted in the interception of legal or otherwise confidential communications, and so-called ‘thematic’ warrants). Secondly, inspectors scrutinised the selected warrants and associated documentation in detail during reading days which preceded the inspections. Thirdly, they identified those warrants, operations or areas of the process which required further information or clarification and arranged to interview relevant operational, legal or technical staff. Where necessary, they examined further documentation or systems relating to those warrants.

185. 970 warrants were examined during the twenty-two interception inspections (sixty-one percent of the number of warrants in force at the end of the year and thirty-two percent of the total of new warrants issued in 2016).

186. According to the report, every interception agency had a different view on what constituted an appropriate retention period for intercepted material and related communications data. There was no period prescribed by the legislation, but the agencies had to consider section 15(3) of RIPA, which provided that the material or data had to be destroyed as soon as retaining it was no longer necessary for any of the authorised purposes in section 15(4). The vast majority of content was reviewed and automatically deleted after a very short period of time unless specific action was taken to retain the content for longer because it was necessary to do so. The retention periods differed within the interception agencies and ranged between thirty days and one year. The retention periods for related communications data also differed within the interception agencies, but ranged between six months and one year.

187. Inspectors made a total of twenty-eight recommendations in their inspection reports, eighteen of which were made in relation to the application process. The majority of the recommendations in this category related to the necessity, proportionality and/or collateral intrusion justifications in the applications; or the handling of legally privileged or otherwise confidential material relating to sensitive professions.

188. The total number of interception errors reported to the Commissioner during 2016 was 108. Key causes of interception errors were over-collection (generally technical software or hardware errors that caused over-collection of intercepted material and related communications data), unauthorised selection/examination, incorrect dissemination, the failure to cancel interception, and the interception of either an incorrect communications address or person.

(b) Acquisition of communications data under Chapter II of RIPA

189. According to the report, police forces and law enforcement agencies were responsible for acquiring ninety-three percent of the total number of items of data in 2016, six percent was acquired by intelligence services and the remaining one percent was acquired by other public authorities, including local authorities. Fifty percent of the data acquired was subscriber information, forty-eight percent was traffic data and two percent service use information. Most of the acquired items of data (eighty-one percent) related to telephony, such as landlines or mobile phones. Internet identifiers, for example email or IP addresses, accounted for fifteen percent of the acquired data and two percent of requests were related to postal identifiers.

190. With regard to the purpose of the request, eighty-three percent of the items of data were acquired for the purpose of preventing or detecting crime or preventing disorder; eleven percent were acquired for the purpose of preventing death or injury or damage to a person's mental health, or of mitigating any injury or damage to a person's physical or mental health; and six percent were acquired in the interests of national security.

191. Furthermore, approximately seventy percent of data requests were for data less than three months old, twenty-five percent aged between three months and one year, and six percent for data over twelve months old. Eighty-one percent of the requests required data for a communications address for periods of three months or less (for example, three months of incoming and outgoing call data for a communications address). Twenty-five percent of all requests were for data relating to a period of less than one day.

192. Twenty-seven percent of submitted applications were returned to the applicant by the Single Point of Contact ("SPoC") for development and a further five percent were declined by the SPoC. Reasons for refusing data applications included: lack of clarity; failure to link the crime to the communications address; and insufficient justification for collateral intrusion. Four percent of submitted applications were returned to applicants by designated persons for further development and one percent was rejected. The main reason for designated persons returning or rejecting applications was that they were not satisfied with the necessity or proportionality justifications given (fifty-two percent). A significant number of applications were returned because designated persons were not satisfied with the overall quality or clarity of the application (twenty-one percent). Other reasons for rejection included the designated persons declaring that they were not independent of the investigation and requesting that the application be forwarded to an independent designated person for consideration (six percent).

193. In 2016 forty-seven public authorities advised that they had made a total of 948 applications that related to persons who were members of

sensitive professions. A significant proportion of these 948 applications were categorised incorrectly (that is, the applicant had recorded a sensitive profession when there was not one). This was usually because the applicant erred on the side of caution, recording a sensitive profession if there was a possibility of one, rather than because they knew that there was one, a fact which provided the Commissioner with “a greater level of assurance that [designated persons] are taking sensitive professions into account when necessary”. Furthermore, according to the Commissioner, most applications relating to members of sensitive professions were submitted because the individual had been a victim of crime or was the suspect in a criminal investigation. In these cases, the profession of the individual was usually not relevant to the investigation, but public authorities showed proper consideration of the sensitive profession by bringing it to the attention of the authorising officer.

194. Having considered the “reportable errors”, the Commissioner noted that the number of serious errors remained very low (0.004%).

G. The Investigatory Powers Act 2016

195. The Investigatory Powers Act 2016 received Royal Assent on 29 November 2016.

196. On 30 December 2016 Part 4 of the 2016 Act, which included a power to issue “retention notices” to telecommunications operators requiring the retention of data, came into force (although not in its entirety). Following a legal challenge by Liberty, the Government conceded that Part 4 of the IPA was, in its current form, inconsistent with the requirements of EU law. Part 4 was not amended and on 27 April 2018 the High Court found Part 4 to be incompatible with fundamental rights in EU law since, in the area of criminal justice, access to retained data was not limited to the purpose of combating “serious crime”; and access to retained data was not subject to prior review by a court or an independent administrative body. The court concluded that the legislation had to be amended by 1 November 2018.

197. On 13 February 2017 the provisions of the IPA relating to the appointment of the Investigatory Powers Commissioner and other Judicial Commissioners came into force. On 3 March 2017, the Government appointed the first Investigatory Powers Commissioner (a judge currently sitting on the Court of Appeal and former justice of the International Criminal Court) for a three-year term and he took up appointment with immediate effect. The newly created Investigatory Powers Commissioners Office (“ICPO”) commenced operations on 8 September 2017 and is ultimately due to consist of around 70 staff (including approximately fifteen judicial commissioners made up of current and recently retired judges of the

High Court, Court of Appeal and Supreme Court, and a technical advisory panel of scientific experts).

198. The remainder of the 2016 Act is not yet in force.

199. In terms of safeguards, when it enters into force in full the Act will require that bulk interception and bulk equipment interference warrants may only be issued where the main purpose of the interception is to acquire intelligence relating to individuals outside the United Kingdom, even where the conduct occurs within the United Kingdom. Similarly, interference with the privacy of persons in the United Kingdom will be permitted only to the extent that it is necessary for that purpose. It will also introduce a “double-lock” for the most intrusive surveillance powers, meaning that a warrant issued by the Secretary of State will also require the approval of one of the appointed Judicial Commissioners. There will also be new protections for journalistic and legally privileged material, including a requirement for judicial authorisation for the acquisition of communications data identifying journalists’ sources; tough sanctions for the misuse of powers, including the creation of new criminal offences; and a right of appeal from the IPT.

200. In addition, the new Act will consolidate and update the powers available to the State to obtain communications and communications data. It will provide an updated framework for the use (by the security and intelligence services, law enforcement and other public authorities) of investigatory powers to obtain communications and communications data. These powers cover the interception of communications, the retention and acquisition of communications data, and equipment interference for obtaining communications and other data. The Act also makes provision relating to the security and intelligence services’ retention and examination of bulk personal datasets.

201. On 23 February 2017 the Home Office launched a public consultation on the five draft codes of practice it intends to issue under the 2016 Act (on the Interception of Communications, Equipment Interference, Bulk Communications Data Acquisition, Retention and Use of Bulk Personal Datasets by the Security and Intelligence Agencies and National Security Notices), which will set out the processes and safeguards governing the use of investigatory powers by public authorities. They will give detail on how the relevant powers should be used, including examples of best practice. They are intended to provide additional clarity and to ensure the highest standards of professionalism and compliance with the relevant legislation. Following the closure of the consultation on 6 April 2017, the draft codes were further amended and Regulations bringing them into force will be laid and debated before Parliament. They will only come into force when they have been debated in both Houses of Parliament and approved by a resolution in both Houses.

H. Relevant international law

1. *The United Nations*

(a) Resolution no. 68/167 on The Right to Privacy in the Digital Age

202. Resolution no. 68/167, adopted by the General Assembly on 18 December 2013, reads as follows:

“The General Assembly,

...

4. *Calls upon* all States:

...

(c) To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;

(d) To establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data ...”

(b) The Constitution of the International Telecommunication Union 1992

203. Articles 33 and 37 of the Constitution provide as follows:

The Right of the Public to Use the International Telecommunication Service

“Member States recognize the right of the public to correspond by means of the international service of public correspondence. The services, the charges and the safeguards shall be the same for all users in each category of correspondence without any priority or preference.
...”

Secrecy of Telecommunications

“1. Member States agree to take all possible measures, compatible with the system of telecommunication used, with a view to ensuring the secrecy of international correspondence.

2. Nevertheless, they reserve the right to communicate such correspondence to the competent authorities in order to ensure the application of their national laws or the execution of international conventions to which they are parties.”

(c) The 2006 Annual Report of the International Law Commission

204. In its 2006 Annual Report the ILC proposed to include the topic “Protection of personal data in the transborder flow of information” in its

long-term programme of work. The Secretariat's supporting report (Annex D) identifies a number of core principles of public international law:

Core principles

"23. A number of core principles are discernible from developments in this field in almost forty-years. Such principles include the following:

Lawful and fair data collection and processing: This principle presupposes that the collection of personal data would be restricted to a necessary minimum. In particular such data should not be obtained unlawfully or through unfair means;

Accuracy: The information quality principle is a qualitative requirement and entails a responsibility that the data be accurate, and necessarily complete and up to date for the purpose intended.

Purpose specification and limitation: This principle establishes the requirement that the purpose for which the data are collected should be specified to the data subject. Data should not be disclosed, made available or otherwise used for purposes other than those specified. It has to be done with the consent or knowledge of the data-subject or under the operation of the law. Any subsequent use is limited to such purpose, or any other that is not incompatible with such purpose. Differences lie in the approaches taken by States. Some jurisdictions perceive the obligation for consent to be *ex ante*.

Proportionality: Proportionality requires that the necessary measure taken should be proportionate to the legitimate claims being pursued.

Transparency: Denotes a general policy of openness regarding developments, practices and policies with respect to protection of personal data.

Individual participation and in particular the right to access: This principle may be the most important for purposes of data protection. The individual should have access to such data; as well as to the possibility of determining whether or not the keeper of the file has data concerning him; to obtain such information or to have it communicated to him in a form, in a manner and at a cost that is reasonable. This accords with the right of an individual to know about the existence of any data file, its contents, to challenge the data and to have it corrected, amended or erased.

Non-discrimination: This principle connotes that data likely to give rise to unlawful and arbitrary discrimination should not be compiled. This includes information collated on racial or ethnic origin, colour, sex life, political opinions, religious, philosophical and other beliefs as well as membership of an association or trade union.

Responsibility: This principle embraces data security; data should be protected by reasonable and appropriate measures to prevent their loss, destruction, unauthorized access, use, modification or disclosure and the keeper of the file should be accountable for it.

Independent supervision and legal sanction: Supervision and sanction require that there should be a mechanism for ensuring due process and accountability. There should be an authority accountable in law for giving effect to the requirements of data protection.

Data equivalency in the case of transborder flow of personal data: This is a principle of compatibility; it is intended to avoid the creation of unjustified obstacles and restrictions to the free flow of data, as long as the circulation is consistent with the standard or deemed adequate for that purpose.

The principle of derogability: This entails power to make exceptions and impose limitations if they are necessary to protect national security, public order, public health or morality or to protect the rights of others."

Derogability

"24. While privacy concerns are of critical importance, such concerns have to be balanced with other value-interests. The privacy values to avoid embarrassment, to

construct intimacy and to protect against misuse associated with the need to protect the individual have to be weighed against other counter-values against individual control over personal information; such as the need not to disrupt the flow of international trade and commerce and the flow of information; the importance of securing the truth, as well as the need to be live in secure environment. There are allowable restrictions and exceptions, for example, with respect to national security, public order (*ordre public*), public health or morality or in order to protect the rights and freedoms of others, as well as the need for effective law enforcement and judicial cooperation in combating crimes at the international level, including the threats posed by international terrorism and organized crime.

25. The processing of personal data must be interpreted in accordance with human rights principles. Accordingly, any of the objectives in the public interest would justify interference with private life if it is (a) in accordance with the law, (b) is necessary in a democratic society for the pursuit of legitimate aims, and (c) is not disproportionate to the objective pursued. The phrase “in accordance with the law” goes beyond to the formalism of having in existence a legal basis in domestic law, it requires that the legal basis be “accessible” and foreseeable”. Foreseeability necessitates sufficiency of precision in formulation of the rule to enable any individual to regulate his conduct.”

2. The Council of Europe

(a) The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981

205. The Convention, which entered into force in respect of the United Kingdom on 1 December 1987, sets out standards for data protection in the sphere of automatic processing of personal data in the public and private sectors. It provides, insofar as relevant:

Preamble

“The member States of the Council of Europe, signatory hereto,

Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms;

Considering that it is desirable to extend the safeguards for everyone’s rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing;

Reaffirming at the same time their commitment to freedom of information regardless of frontiers;

Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples,

Have agreed as follows:”

Article 1 – Object and purpose

“The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and

94 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him (“data protection”).

...”

Article 8 – Additional safeguards for the data subject

“Any person shall be enabled:

a. to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;

b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;

c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;

d. to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.”

Article 9 – Exceptions and restrictions

“1. No exception to the provisions of Articles 5, 6 and 8 of this Convention shall be allowed except within the limits defined in this article.

2. Derogation from the provisions of Articles 5, 6 and 8 of this Convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:

a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;

b. protecting the data subject or the rights and freedoms of others.

...”

Article 10 – Sanctions and remedies

“Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.”

206. The Explanatory Report explains that:

Article 9 – Exceptions and restrictions

“55. Exceptions to the basic principles for data protection are limited to those which are necessary for the protection of fundamental values in a democratic society. The text of the second paragraph of this article has been modelled after that of the second paragraphs of Articles 6, 8, 10 and 11 of the European Human Rights Convention. It is clear from the decisions of the Commission and the Court of Human Rights relating to the concept of “necessary measures” that the criteria for this concept cannot be laid down for all countries and all times, but should be considered in the light of the given situation in each country.

56. Littera a in paragraph 2 lists the major interests of the State which may require exceptions. These exceptions are very specific in order to avoid that, with regard to the general application of the convention, States would have an unduly wide leeway.

States retain, under Article 16, the possibility to refuse application of the convention in individual cases for important reasons, which include those enumerated in Article 9.

The notion of "State security" should be understood in the traditional sense of protecting national sovereignty against internal or external threats, including the protection of the international relations of the State."

(b) The Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows of 8 November 2001 (CETS No. 181)

207. The Protocol, which has not been ratified by the United Kingdom, provides, insofar as relevant:

Article 1 – Supervisory authorities

"1. Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the measures in its domestic law giving effect to the principles stated in Chapters II and III of the Convention and in this Protocol.

2. a. To this end, the said authorities shall have, in particular, powers of investigation and intervention, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of provisions of domestic law giving effect to the principles mentioned in paragraph 1 of Article 1 of this Protocol.

b. Each supervisory authority shall hear claims lodged by any person concerning the protection of his/her rights and fundamental freedoms with regard to the processing of personal data within its competence.

3. The supervisory authorities shall exercise their functions in complete independence.

4. Decisions of the supervisory authorities, which give rise to complaints, may be appealed against through the courts.

..."

Article 2 – Transborder flows of personal data to a recipient which is not subject to the jurisdiction of a Party to the Convention

"1. Each Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an adequate level of protection for the intended data transfer.

2. By way of derogation from paragraph 1 of Article 2 of this Protocol, each Party may allow for the transfer of personal data:

- a. if domestic law provides for it because of:
 - specific interests of the data subject, or

96 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

– legitimate prevailing interests, especially important public interests, or

b. if safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law.”

(c) Recommendation of the Committee of Ministers on the protection of personal data in the area of telecommunication services

208. This Recommendation (No. R (95) 4 of the Committee of Ministers), which was adopted on 7 February 1995, reads, insofar as relevant, as follows:

“2.4. Interference by public authorities with the content of a communication, including the use of listening or tapping devices or other means of surveillance or interception of communications, must be carried out only when this is provided for by law and constitutes a necessary measure in a democratic society in the interests of:

a. protecting state security, public safety, the monetary interests of the state or the suppression of criminal offences;

b. protecting the data subject or the rights and freedoms of others.

2.5. In the case of interference by public authorities with the content of a communication, domestic law should regulate:

a. the exercise of the data subject’s rights of access and rectification;

b. in what circumstances the responsible public authorities are entitled to refuse to provide information to the person concerned, or delay providing it;

c. storage or destruction of such data.

If a network operator or service provider is instructed by a public authority to effect an interference, the data so collected should be communicated only to the body designated in the authorisation for that interference.”

(d) The 2001 (Budapest) Convention on Cybercrime

209. The Convention provides, insofar as relevant:

Preamble

“The member States of the Council of Europe and the other States signatory hereto,

...

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT 97

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

...

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems.”

Article 2 – Illegal access

“Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.”

Article 3 – Illegal interception

“Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.”

Article 4 – Data interference

“1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

...”

Article 15 – Conditions and safeguards

“1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.”

210. The Explanatory Report explains that:

“38. A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self-defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised. Specific examples of such exceptions from criminalisation are provided in relation to specific offences in the corresponding text of the Explanatory Memorandum below. It is left to the Parties to determine how such exemptions are implemented within their domestic legal systems (under criminal law or otherwise).

...

“58. For criminal liability to attach, the illegal interception must be committed "intentionally", and "without right". The act is justified, for example, if the intercepting person has the right to do so, if he acts on the instructions or by authorisation of the participants of the transmission (including authorised testing or protection activities agreed to by the participants), or if surveillance is lawfully authorised in the interests of national security or the detection of offences by investigating authorities.”

(e) The 2015 Report of the European Commission for Democracy through Law (“the Venice Commission”) on the Democratic Oversight of Signals Intelligence Agencies

211. The Venice Commission noted, at the outset, the value that bulk interception could have for security operations, since it enabled the security services to adopt a proactive approach, looking for hitherto unknown dangers rather than investigating known ones. However, it also noted that intercepting bulk data in transmission, or requirements that telecommunications companies store and then provide telecommunications content data or metadata to law-enforcement or security agencies involved an interference with the privacy and other human rights of a large proportion of the population of the world. In this regard, the Venice Commission considered that the main interference with privacy occurred when stored personal data was accessed and/or processed by the agencies. For this reason, the computer analysis (usually with the help of selectors) was one of the important stages for balancing personal integrity concerns against other interests.

212. According to the report, the two most significant safeguards were the authorisation process (of collection and access) and the oversight process. It was clear from the Court’s case-law that the latter must be performed by an independent, external body. While the Court had a preference for judicial authorisation, it had not found this to be a necessary requirement. Rather, the system had to be assessed as a whole, and where independent controls were absent at the authorisation stage, particularly strong safeguards had to exist at the oversight stage. In this regard, the Venice Commission considered the example of the system in the United States, where authorisation was given by the Foreign Intelligence Surveillance Court. However, it noted that despite the existence of judicial authorisation, the lack of independent oversight of the court’s conditions was problematic.

213. Similarly, the Commission observed that notification of the subject of surveillance was not an absolute requirement of Article 8 of the Convention. In this regard, a general complaints procedure to an independent oversight body could compensate for non-notification.

214. The report also considered internal controls to be a “primary safeguard”. In this regard, recruitment and training were key issues; in addition, it was important for the agencies to build in respect for privacy and other human rights when promulgating internal rules.

215. The report also considered the position of journalists. It accepted that they were a group which required special protection, since searching their contacts could reveal their sources (and the risk of discovery could be a powerful disincentive to whistle-blowers). Nevertheless, it considered there to be no absolute prohibition on searching the contacts of journalists, provided that there were very strong reasons for doing so. It acknowledged,

100 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

however, that the journalistic profession was not one which was easily identified, since NGOs were also engaged in building public opinion and even bloggers could claim to be entitled to equivalent protections.

216. Finally, the report briefly considered the issue of intelligence sharing, and in particular the risk that States could thereby circumvent stronger domestic surveillance procedures and/or any legal limits which their agencies might be subject to as regards domestic intelligence operations. It considered that a suitable safeguard would be to provide that the bulk material transferred could only be searched if all the material requirements of a national search were fulfilled and this was duly authorised in the same way as a search of bulk material obtained by the signals intelligence agency using its own techniques.

I. European Union law

1. Charter of Fundamental Rights of the European Union

217. Articles 7, 8 and 11 of the Charter provide as follows:

Article 7 – Respect for private and family life

“Everyone has the right to respect for his or her private and family life, home and communications.”

Article 8 – Protection of personal data

“1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which have been collected concerning him or her, and the right to have them rectified.

3. Compliance with these rules shall be subject to control by an independent authority.”

Article 11 – Freedom of expression and information

“1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

2. The freedom and pluralism of the media shall be respected.”

2. EU directives and regulations relating to protection and processing of personal data

218. The Data Protection Directive (Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data), adopted on 24 October 1995, regulated for many years the protection and processing of personal data within the European Union. As the activities of Member States regarding public safety,

defence and State security fall outside the scope of Community law, the Directive did not apply to these activities (Article 3(2)).

219. The General Data Protection Regulation, adopted in April 2016, superseded the Data Protection Directive and became enforceable on 25 May 2018. The regulation, which is directly applicable in Member States¹, contains provisions and requirements pertaining to the processing of personally identifiable information of data subjects inside the European Union, and applies to all enterprises, regardless of location, that are doing business with the European Economic Area. Business processes that handle personal data must be built with data protection by design and by default, meaning that personal data must be stored using pseudonymisation or full anonymisation, and use the highest-possible privacy settings by default, so that the data is not available publicly without explicit consent, and cannot be used to identify a subject without additional information stored separately. No personal data may be processed unless it is done under a lawful basis specified by the regulation, or if the data controller or processor has received explicit, opt-in consent from the data's owner. The data owner has the right to revoke this permission at any time.

220. A processor of personal data must clearly disclose any data collection, declare the lawful basis and purpose for data processing, how long data is being retained, and if it is being shared with any third-parties or outside of the EU. Users have the right to request a portable copy of the data collected by a processor in a common format, and the right to have their data erased under certain circumstances. Public authorities, and businesses whose core activities centre around regular or systematic processing of personal data, are required to employ a data protection officer (DPO), who is responsible for managing compliance with the GDPR. Businesses must report any data breaches within 72 hours if they have an adverse effect on user privacy.

221. The Privacy and Electronic Communications Directive (Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector), adopted on 12 July 2002, states, in recitals 2 and 11:

“(2) This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the Charter of fundamental rights of the European Union. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter.

(11) Like Directive 95/46/EC, this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the

¹ As the United Kingdom is leaving the European Union in 2019, it granted royal assent to the Data Protection Act 2018 on 23 May 2018, which contains equivalent regulations and protections.

measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.”

222. The Directive further provides, insofar as relevant:

Article 1 – Scope and aim

“1. This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

2. The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.

3. This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.”

Article 15 – Application of certain provisions of Directive 95/46/EC

“1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, *inter alia*, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.”

223. On 15 March 2006 the Data Retention Directive (Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and

amending Directive 2002/58/EC) was adopted. It provided, insofar as relevant:

Article 1 - Subject matter and scope

“1. This Directive aims to harmonise Member States’ provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.

2. This Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network.”

Article 3 – Obligation to retain data

“1. By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.”

3. *Relevant case-law of the Court of Justice of the European Union (“CJEU”)*

(a) *Digital Rights Ireland v. Minister for Communications, Marine and Natural Resources and Others and Seitinger and Others (Cases C-293/12 and C-594/12; ECLI:EU:C:2014:238)*

224. In a judgment of 8 April 2014 the Court of Justice of the European Union (“the CJEU”) declared invalid the Data Retention Directive 2006/24/EC laying down the obligation on the providers of publicly available electronic communication services or of public communications networks to retain all traffic and location data for periods from six months to two years, in order to ensure that the data was available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. The CJEU noted that, even though the directive did not permit the retention of the content of the communication, the traffic and location data covered by it might allow very precise conclusions to be drawn concerning the private lives of the persons whose data had been retained. Accordingly, the obligation to retain the data constituted in itself an interference with the right to respect for private life and communications guaranteed by Article 7 of the Charter of Fundamental Rights of the EU and the right to protection of personal data under Article 8 of the Charter.

225. The access of the competent national authorities to the data constituted a further interference with those fundamental rights, which the CJEU considered to be “particularly serious”. The fact that data was retained and subsequently used without the subscriber or registered user being informed was, according to the CJEU, likely to generate in the minds of the persons concerned the feeling that their private lives were the subject of constant surveillance. The interference satisfied an objective of general interest, namely to contribute to the fight against serious crime and terrorism and thus, ultimately, to public security. However, it failed to satisfy the requirement of proportionality.

226. Firstly, the directive covered, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime. It therefore entailed an interference with the fundamental rights of practically the entire European population. It applied even to persons for whom there was no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime.

227. Secondly, the directive did not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. By simply referring, in a general manner, to serious crime, as defined by each Member State in its national law, the directive failed to lay down any objective criterion by which to determine which offences might be considered to be sufficiently serious to justify such an extensive interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. Above all, the access by the competent national authorities to the data retained was not made dependent on a prior review carried out by a court or by an independent administrative body whose decision sought to limit access to the data and their use to what was strictly necessary for the purpose of attaining the objective pursued.

228. Thirdly, the directive required that all data be retained for a period of at least six months, without any distinction being made between the categories of data on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned. The CJEU concluded that the directive entailed a wide-ranging and particularly serious interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, without such an interference being precisely circumscribed by provisions to ensure that it was actually limited to what was strictly necessary. The CJEU also noted that the directive did not provide for sufficient safeguards, by means of technical and organisational measures, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of those data.

(b) *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* (Cases C-203/15 and C-698/15; ECLI:EU:C:2016:970)

229. In *Secretary of State for the Home Department v. Watson and Others*, the applicants had sought judicial review of the legality of section 1 of the Data Retention and Investigatory Powers Act 2014 (“DRIPA”), pursuant to which the Secretary of State could require a public telecommunications operator to retain relevant communications data if he considered it necessary and proportionate for one or more of the purposes falling within paragraphs (a) to (h) of section 22(2) of RIPA. The applicants claimed, *inter alia*, that section 1 was incompatible with Articles 7 and 8 of the Charter and Article 8 of the Convention.

230. By judgment of 17 July 2015, the High Court held that the *Digital Rights* judgment laid down “mandatory requirements of EU law” applicable to the legislation of Member States on the retention of communications data and access to such data. Since the CJEU, in that judgment, held that Directive 2006/24 was incompatible with the principle of proportionality, national legislation containing the same provisions as that directive could, equally, not be compatible with that principle. In fact, it followed from the underlying logic of the *Digital Rights* judgment that legislation that established a general body of rules for the retention of communications data was in breach of the rights guaranteed in Articles 7 and 8 of the Charter, unless that legislation was complemented by a body of rules for access to the data, defined by national law, which provides sufficient safeguards to protect those rights. Accordingly, section 1 of DRIPA was not compatible with Articles 7 and 8 of the Charter as it did not lay down clear and precise rules providing for access to and use of retained data and access to that data was not made dependent on prior review by a court or an independent administrative body.

231. On appeal by the Secretary of State, the Court of Appeal sought a preliminary ruling from the CJEU.

232. Before the CJEU this case was joined with the request for a preliminary ruling from the Kammarrätten i Stockholm in Case C-203/15 *Tele2 Sverige AB v Post- och telestyrelsen*. Following an oral hearing in which some fifteen EU Member States intervened, the CJEU gave judgment on 21 December 2016. The CJEU held that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, had to be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, was not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative

authority, and where there is no requirement that the data concerned should be retained within the European Union.

233. The CJEU declared the Court of Appeal's question whether the protection afforded by Articles 7 and 8 of the Charter was wider than that guaranteed by Article 8 of the Convention inadmissible.

234. Following the handing down of the CJEU's judgment, the case was relisted before the Court of Appeal. On 31 January 2018 it granted declaratory relief in the following terms: that section 1 of DRIPA was inconsistent with EU law to the extent that it permitted access to retained data where the object pursued by access was not restricted solely to fighting serious crime; or where access was not subject to prior review by a court or independent administrative authority.

(c) *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service and Secret Intelligence Service* (IPT/15/110/CH; EU OJ C 22, 22.1.2018, p. 29–30)

235. On 8 September 2017 the IPT gave judgment in the case of *Privacy International*, which concerned the acquisition by the agencies of Bulk Communications Data under section 94 of the Telecommunications Act 1984 (a different regime from those which form the subject of the present complaints) and Bulk Personal Data. The IPT found that, following their avowal, the regimes were compliant with Article 8 of the Convention. However, it identified the following four requirements which appeared to flow from the CJEU judgment in *Watson and Others* and which seemed to go beyond the requirements of Article 8 of the Convention: a restriction on non-targeted access to bulk data; a need for prior authorisation (save in cases of validly established emergency) before data could be accessed; provision for subsequent notification of those affected; and the retention of all data within the European Union.

236. On 30 October 2017 the IPT made a request to the CJEU for a preliminary ruling clarifying the extent to which the *Watson* requirements could apply where the bulk acquisition and automated processing techniques were necessary to protect national security. In doing so, it expressed serious concern that if the *Watson* requirements were to apply to measures taken to safeguard national security, they would frustrate them and put the national security of Member States at risk. In particular, it noted the benefits of bulk acquisition in the context of national security (referring to the Bulk Powers Review – see paragraphs 173-176 above); the risk that the need for prior authorisation could undermine the agencies' ability to tackle the threat to national security; the danger and impracticality of implementing a requirement to give notice in respect of the acquisition or use of a bulk database, especially where national security was at stake; and

the impact an absolute bar on the transfer of data outside the European Union could have on Member States' treaty obligations.

THE LAW

I. EXHAUSTION OF DOMESTIC REMEDIES

237. The Government submitted that the applicants in the first and second of the joined cases had not exhausted domestic remedies within the meaning of Article 35 § 1 of the Convention, which provides as follows:

“1. The Court may only deal with the matter after all domestic remedies have been exhausted, according to the generally recognised rules of international law, and within a period of six months from the date on which the final decision was taken.”

A. The parties' submissions

1. *The Government*

238. The Government argued that the applicants in the first and second of the joined cases had not exhausted domestic remedies as they had failed to raise their complaints before the IPT. The IPT was a bespoke domestic tribunal set up for the very purpose of investigating, considering and ruling on the issues now raised before this Court. In *Kennedy v. the United Kingdom*, no. 26839/05, 18 May 2010 the Court held that the IPT was Article 6 compliant and, as could be seen from the *Liberty* proceedings, it was capable of providing redress. Furthermore, it was advantageous for the Court to have the benefit of a detailed assessment of the operation of the relevant domestic legal regime by a bespoke domestic tribunal with an understanding of that system. That was especially so where, as in the case at hand, domestic law was not only complex, but also involved an assessment of issues of necessity and proportionality which would be particularly difficult to undertake without a proper determination at national level of facts material to the balance between the rights of the individual and the interests of the community as a whole.

239. As for the effectiveness of the IPT as a domestic remedy, the Government noted that it was “one of the most far-reaching systems of judicial oversight over intelligence matters in the world”, with broad jurisdiction and remedial powers. It produced open judgments to the extent that it could do so consistently with the public interest. It could investigate and consider in closed session any sensitive material that was relevant to the complaints and produce decisions having regard to that material. On account of its ability to assess and evaluate the adequacy of the internal safeguards, it was in a “special position” to make a proper assessment of

proportionality. In the present case, the applicants' complaints under Articles 8 and 10 of the Convention focussed on the alleged lack of publicly available safeguards and proportionality, and the IPT had the jurisdiction and requisite powers to deal with all of those complaints. It could make clear the extent to which the relevant domestic regime was compatible with the Convention and, if it was not compatible, it could identify the respects in which it was deficient. If there was a lack of foreseeability, it could identify with precision the respects in which the applicable safeguards were not – but should be – public, which, in turn, meant that those aspects of the regime could be remedied by the Government with further disclosure and/or amendments to the Code of Practice. Finally, where proportionality was in issue, it could, through its ability to consider relevant intelligence material in closed proceedings, provide an effective remedy by ordering the quashing of section 8(4) warrants and ordering the destruction of data.

240. Finally, in relation to the IPT's more general declaratory jurisdiction, the Government argued that there was no deficit in Convention terms. On the contrary, it could and did rule on the general lawfulness of regimes about which complaints were made and if it concluded that a regime was contrary to the Convention, it would so state. Furthermore, the Government's reaction to such findings had been consistent. As could be seen from the response to the *Liberty* and *Belhadj* determinations (see paragraphs 92-94 above), it had ensured that any defects were rectified and dealt with. Therefore, even though it has no jurisdiction to make a Declaration of Incompatibility under section 4 of the Human Rights Act 1998, on the facts a finding of incompatibility would be an effective trigger for the necessary changes to ensure Convention compatibility. In light of both this fact, and the Court's increasing emphasis on subsidiarity, the Government contended that the position had moved on since *Kennedy*, in which the Court did not accept that the IPT had provided the applicant with an effective remedy for his general complaint about the Convention compliance of section 8(1) of RIPA.

2. *The applicants*

241. The applicants in the first and second of the joined cases submitted that they had done all that was required of them in terms of domestic remedies. While they accepted that they did not file complaints with the IPT before lodging their applications with this Court, they had not done so in reliance on the Court's findings in *Kennedy*; namely, that a claim before the IPT was not necessary in order for a general challenge to be brought against the United Kingdom's domestic framework. Although they accepted that it was always open to the Court to reconsider whether a domestic avenue of complaint provided an effective remedy, it had held that an applicant could only be required to make use of a remedy that had developed since the application was lodged if they could still make use of the remedy and it

would not be unjust to declare the application admissible (*Campbell and Fell v. the United Kingdom*, 28 June 1984, §§ 62-63, Series A no. 80).

242. In any event, the applicants argued that there had been no change of circumstances such as would make the IPT an effective remedy. In particular, they relied upon the arguments made by the applicants in the third of the joined cases in support of their Article 6 complaint, and further noted that the IPT could not make a Declaration of Incompatibility. The latter in any case did not constitute an effective remedy, since it did not result in the invalidation of the impugned legislation).

B. The submissions of the third party

243. In its third party intervention, the European Network of National Human Rights Institutions (“ENNHRI”) submitted that the international legal framework, including the International Covenant on Civil and Political Rights (“ICCPR”) and the American Convention on Human Rights (“ACHR”), and case-law supported the contention that domestic remedies did not have to be followed if they were not capable of providing an effective remedy.

C. The Court’s assessment

1. General principles

244. It is a fundamental feature of the machinery of protection established by the Convention that it is subsidiary to the national systems safeguarding human rights. This Court is concerned with the supervision of the implementation by Contracting States of their obligations under the Convention. It should not take on the role of Contracting States, whose responsibility it is to ensure that the fundamental rights and freedoms enshrined therein are respected and protected on a domestic level (*Vučković and Others v. Serbia* (preliminary objection) [GC], nos. 17153/11 and 29 others, § 69, 25 March 2014). However, the application of the rule must make due allowance for the fact that it is being applied in the context of machinery for the protection of human rights that the Contracting Parties have agreed to set up and it must therefore be applied with some degree of flexibility and without excessive formalism (see *Vučković and Others*, cited above, § 76; see also *Akdivar and Others v. Turkey*, 16 September 1996, § 69, *Reports of Judgments and Decisions* 1996-IV and *Gough v. the United Kingdom*, no. 49327/11, § 140, 28 October 2014).

245. States are dispensed from answering before an international body for their acts before they have had an opportunity to put matters right through their own legal system, and those who wish to invoke the supervisory jurisdiction of the Court as concerns complaints against a State

are thus obliged to use first the remedies provided by the national legal system (see, among many authorities, *Vučković and Others*, cited above, § 70 and *Akdivar and Others*, cited above, § 65). The Court is not a court of first instance; it does not have the capacity, nor is it appropriate to its function as an international court, to adjudicate on cases which require the finding of basic facts, which should, as a matter of principle and effective practice, be the domain of domestic jurisdiction (see *Demopoulos and Others v. Turkey* (dec.) [GC], nos. 46113/99, 3843/02, 13751/02, 13466/03, 10200/04, 14163/04, 19993/04 and 21819/04, § 69, ECHR 2010). Similarly, in cases requiring the balancing of conflicting interests under Articles 8 and 10 of the Convention it is particularly important that the domestic courts are first given the opportunity to strike the “complex and delicate” balance between the competing interests at stake. Those courts are in principle better placed than this Court to make such an assessment and, as a consequence, their conclusions will be central to its own consideration of the issue (*MGN Limited v. the United Kingdom*, no. 39401/04, §§ 140-155, 18 January 2011; *Palomo Sánchez and Others v. Spain* [GC], nos. 28955/06, 28957/06, 28959/06 and 28964/06, § 57, 12 September 2011; *Axel Springer AG v. Germany* [GC], no. 39954/08, §§ 85-88, 7 February 2012; *Courtney v. Ireland* (dec), no. 69558/10, 18 December 2012; and *Charron and Merle-Montet v. France* (dec), no. 22612/15, § 30, 16 January 2018).

246. The obligation to exhaust domestic remedies therefore requires an applicant to make normal use of remedies which are available and sufficient in respect of his or her Convention grievances. The existence of the remedies in question must be sufficiently certain not only in theory but in practice, failing which they will lack the requisite accessibility and effectiveness (see *Vučković and Others*, cited above, § 71 and *Akdivar and Others*, cited above, § 66).

247. There is, however, no obligation to have recourse to remedies which are inadequate or ineffective. To be effective, a remedy must be capable of remedying directly the impugned state of affairs and must offer reasonable prospects of success (see *Vučković and Others*, cited above, § 73 and *Sejdovic v. Italy* [GC], no. 56581/00, § 46, ECHR 2006-II). The existence of mere doubts as to the prospects of success of a particular remedy which is not obviously futile is not a valid reason for failing to exhaust that avenue of redress (see *Vučković and Others*, cited above, § 74 and *Scoppola v. Italy (no. 2)* [GC], no. 10249/03, § 70, 17 September 2009).

248. As regards the burden of proof, it is incumbent on the Government claiming non-exhaustion to satisfy the Court that the remedy was an effective one, available in theory and in practice at the relevant time. Once this burden has been satisfied, it falls to the applicant to establish that the remedy advanced by the Government was in fact exhausted, or was for some reason inadequate and ineffective in the particular circumstances of

the case, or that there existed special circumstances absolving him or her from this requirement (see *Vučković and Others*, cited above, § 77; *McFarlane v. Ireland* [GC], no. 31333/06, § 107, 10 September 2010; *Demopoulos and Others*, cited above, § 69; and *Akdivar and Others*, cited above, § 68).

249. Where an applicant is challenging the general legal framework for secret surveillance measures, the Court has identified the availability of an effective domestic remedy as a relevant factor in determining whether that applicant was a “victim” of the alleged violation, since, in the absence of such a remedy, widespread suspicion and concern among the general public that secret surveillance powers were being abused might be justified (*Roman Zakharov v. Russia* [GC], no. 47143/06, § 171, ECHR 2015).

2. *Application of those principles to the case at hand*

250. The IPT is a specialist tribunal with sole jurisdiction to hear allegations of wrongful interference with communications as a result of conduct covered by RIPA (see paragraph 124 above). The Court of Appeal has recently observed that the IPT is “a judicial body of like standing and authority to the High Court” and that “[t]he quality of the membership of the IPT in terms of judicial expertise and independence is very high” (see paragraph 135 above). Its members must hold or have held high judicial office or be a qualified lawyer of at least ten years’ standing (see paragraph 123 above), and in the present case it was composed of two High Court Judges (including the President), a Circuit Judge and two senior barristers (see paragraph 24 above). It has jurisdiction to investigate any complaint that a person’s communications have been intercepted (see paragraph 124 above). In conducting such an investigation, the IPT will generally proceed on the assumption that the facts asserted by the applicant are true and then, acting upon that assumption, decide whether they would constitute lawful or unlawful conduct. In doing so, the IPT considers both the generic compliance of the relevant interception regime (on the basis of assuming there to have been an interception as alleged) as well as, at a subsequent stage, the specific question whether the individual applicant’s rights have, in fact, been breached. Those involved in the authorisation and execution of an intercept warrant are required to disclose to the IPT all the documents it may require, including “below the waterline” documents which could not be made public for reasons of national security (see paragraph 127 above), irrespective of whether those documents support or undermine their defence. The IPT has discretion to hold oral hearings, in public, where possible (see paragraphs 131, 138 and 139 above) and, in closed proceedings it may appoint Counsel to the Tribunal to make submissions on behalf of claimants who cannot be represented (see paragraph 142 above). When it determines a complaint the IPT has the power to award compensation and make any other order it sees fit, including

quashing or cancelling any warrant and requiring the destruction of any records (see paragraph 128 above). In considering the complaint brought by the applicants in the third of the joined cases (“the *Liberty* proceedings”), the IPT used all of these powers for the benefit of the applicants.

251. The Court considered the role of the IPT in secret surveillance cases in *Kennedy* (cited above), decided in 2010. In that case the applicant complained that his communications had been intercepted pursuant to a targeted warrant authorised under section 8(1) of RIPA (the specific complaint), and that the targeted interception regime under section 8(1) was not compliant with Article 8 of the Convention (the general compliance complaint). The Court held that the proceedings before the IPT had been Article 6 compliant, since any procedural restrictions were proportionate to the need to keep secret sensitive and confidential information and did not impair the very essence of the applicant’s right to a fair trial. With regard to the IPT’s effectiveness as a remedy, it acknowledged that Article 35 § 1 had “a special significance in the context of secret surveillance given the extensive powers of the IPT to investigate complaints before it and to access confidential information”. It considered these extensive powers to be relevant to the applicant’s specific complaint as it had required a factual investigation into whether his communications had been intercepted. However, it was not persuaded of their relevance to the general compliance complaint, since it was a legal challenge and, having already decided the specific complaint, it was unlikely that the IPT could further elucidate the general operation of the surveillance regime and applicable safeguards, such as would assist the Court in its consideration of the compliance of the regime with the Convention. While it accepted that the IPT could consider a complaint about the general compliance of a surveillance regime with the Convention and, if necessary, make a finding of incompatibility, the Government had not addressed in their submissions how such a finding would benefit the applicant, given that it did not appear to give rise to a binding obligation on the State to remedy the incompatibility.

252. Although in *Kennedy* the Court distinguished between a specific and general complaint, it is clear from its more recent case-law that while the two complaints are indeed distinct, they are nevertheless connected. In *Roman Zakharov* the Court identified the availability of an effective domestic remedy to a person who suspects that he or she was subjected to secret surveillance (in other words, an effective domestic remedy for a specific complaint) as a relevant factor in determining whether that person was a “victim” in respect of a complaint challenging the general legal framework for secret surveillance, since, in the absence of such a remedy, widespread suspicion and concern among the general public that secret surveillance powers were being abused might be justified (*Roman Zakharov*, cited above, § 171). In view of the significance the Court has attached to the existence of such a domestic remedy, it would be

problematic if applicants were not required to use it before making either a specific or general complaint to this Court. The Court should not have to consider a challenge to a legislative regime *in abstracto* when the applicants had a domestic forum in which they could have challenged at the very least the possible application of those measures to them.

253. In any event, the IPT's ruling in Mr Kennedy's case came very early in the Tribunal's history. In fact, Mr Kennedy's application, together with an application lodged by British and Irish Rights Watch, was the first time that the IPT sat in public. It was in the context of those applications that it gave its defining ruling on preliminary issues of law and established its current practice (see paragraphs 136-141 above). For the reasons set out below, the Court considers that in view both of the manner in which the IPT has exercised its powers in the fifteen years that have elapsed since that ruling, and the very real impact its judgments have had on domestic law and practice, the concerns expressed by the Court in *Kennedy* about its effectiveness as a remedy for complaints about the general compliance of a secret surveillance regime are no longer valid.

254. First, in *Kennedy* the IPT had fully examined Mr Kennedy's specific complaint about the interception of his communications. The Court was solely concerned with whether an examination of the general complaint could have provided additional clarification. Unlike the present case, therefore, the Court was not being called upon to consider the general complaint entirely *in abstracto*.

255. Secondly, an examination of the IPT's extensive post-*Kennedy* case-law demonstrates the important role that it can and does play in analysing and elucidating the general operation of secret surveillance regimes. For example, in *B v. the Security Services*, Case No IPT/03/01/CH, 21 March 2004 the IPT considered, as a preliminary issue of law, whether the Secretary of State's "neither confirm nor deny" policy was compatible with Article 8 of the Convention. Similarly, in *A Complaint of Surveillance*, Case No IPT/A1/2013, 24 July 2013 the IPT provided elucidation on the meaning of the term "surveillance" in Part II of RIPA. Moreover, given the "secret" nature of most surveillance regimes, the scope of their operation will not always be evident from the "above the waterline" material. For example, in the *Liberty* proceedings the IPT played a crucial role first in identifying those aspects of the surveillance regimes which could and should be further elucidated, and then recommending the disclosure of certain "below the waterline" arrangements in order to achieve this goal. It could therefore be said that the IPT, as the only tribunal with jurisdiction to obtain and review "below the waterline" material, is not only the sole body capable of elucidating the general operation of a surveillance regime; it is also the sole body capable of determining whether that regime requires further elucidation.

256. This “elucidatory” role is of invaluable assistance to the Court when it is considering the compliance of a secret surveillance regime with the Convention. The Court has repeatedly stated that it is not its role to determine questions of fact or to interpret domestic law. That is especially so where domestic law is complex and, for reasons of national security, the State is not at liberty to disclose relevant information to it. Given the confidential nature of the relevant documentation, were applicants to lodge complaints about secret surveillance with this Court without first raising them before the IPT, this Court would either have to become the primary fact-finder in such cases, or it would have to assess necessity and proportionality in a factual vacuum. This difficulty is particularly apparent in respect of those complaints not considered by the IPT in the *Liberty* proceedings; in particular, the Chapter II complaint and the complaint about the receipt of non-intercept material from foreign intelligence services. The Court has before it very limited information about the scope and operation of these regimes and it could therefore only consider these complaints if it were either to accept the applicants’ allegations as fact, or to attempt to conduct its own fact-finding exercise. In such cases, therefore, it is particularly important that the domestic courts, which have access to the confidential documentation, first strike the “complex and delicate balance” between the competing interests at stake (see paragraph 245 above).

257. Consequently, on the basis of the information submitted to it, the Court considers that the IPT can – and regularly does – elucidate the general operation of surveillance regimes, including in cases where such elucidation is considered necessary to ensure the regime’s Convention compliance.

258. Furthermore, from the information submitted in the present case it would appear that where the IPT has found a surveillance regime to be incompatible with the Convention, the Government have ensured that any defects are rectified and dealt with. In the *Liberty* proceedings, once the IPT had identified which of the “below the waterline” arrangements could and should be made public in order for the intelligence sharing regime to be Convention compliant, the Government agreed to the proposed disclosure (“the 9 October disclosure”) and the disclosed material was subsequently added to the amended Code of Practice (see paragraphs 26-30 above). In addition, having found that there had been a breach of Article 8 of the Convention by virtue of the fact that email communications of Amnesty International, which had been intercepted and accessed “lawfully and proportionately”, had nevertheless been retained for longer than was permitted under GCHQ’s internal policies, the IPT ordered GCHQ to destroy the communications within seven days, and to provide a closed report within fourteen days confirming their destruction (see paragraph 54 above).

259. Similarly, in the *Belhadj* case the Government conceded that from January 2010 the regime for the interception, obtaining, analysis, use,

disclosure and destruction of legally privileged material had not been in accordance with the law for the purposes of Article 8 § 2 of the Convention and was accordingly unlawful. As a consequence, the Security Service and GCHQ confirmed that they would work in the forthcoming weeks to review their policies and procedures (see paragraph 93 above).

260. In addition, in *News Group and Others v. The Commissioner of Police of the Metropolis* the IPT found that the regime under Chapter II of RIPA (for the acquisition of communications data) did not contain effective safeguards to protect Article 10 rights. Although the IPT could not award any remedy in respect of the failure to provide adequate safeguards, as this did not in itself render the authorisations for the acquisition of communications data unlawful, in March 2015 the 2007 ACD Code of Practice was replaced by a new code with enhanced safeguards in respect of applications for communications data designed to identify a journalist's source (see paragraphs 118-120 above). The applicants in that case subsequently lodged a complaint under Article 10 of the Convention with this Court; however, in a recent decision the Court declared the complaint inadmissible as it found that the applicants had not suffered a "significant disadvantage" within the meaning of Article 35 § 3 (b) of the Convention (see *Anthony France and Others v. the United Kingdom* (dec.), nos. 25357/16, 25514/16, 25552/16 and 25597/16, 26 September 2016). In particular, the Court observed that "the applicants have benefitted from a thorough and comprehensive judgment from the IPT, which clearly sets out all the aspects of the interference with their rights". Furthermore, although "the IPT could not find that there had been a violation of their rights, it nonetheless made a clear statement that their rights had been infringed" and a change in the law subsequently occurred (see *Anthony France and Others*, cited above, §§ 43-46).

261. Finally, to cite an earlier example, in *Paton and Others v. Poole Borough Council*, Case Nos IPT/09/01/C, IPT/09/02/C, IPT/09/03/C, IPT/09/04/C and IPT/09/05/C, 29 July 2010, the IPT found that surveillance carried out by a local authority was both unlawful and in breach of Article 8 of the Convention as it was not for the permitted purpose and was neither necessary nor proportionate. While the IPT made no findings regarding the Convention compliance of the regime as a whole, the case was highly publicised and fed into a general public debate about the surveillance powers of local councils. Very shortly after the judgment was handed down, the Government announced that there was to be a review of RIPA which would cover its use by local authorities. Two years later RIPA was amended to restrict the power of local authorities to conduct surveillance.

262. Therefore, while the evidence submitted by the Government may not yet demonstrate the existence of a "binding obligation" requiring it to remedy any incompatibility identified by the IPT, in light of the IPT's "special significance" in secret surveillance cases which arises from its

“extensive powers ... to investigate complaints before it and to access confidential information” (see *Kennedy*, cited above, § 110) the Court would nevertheless accept that the practice of giving effect to its findings on the incompatibility of domestic law with the Convention is sufficiently certain for it to be satisfied as to the effectiveness of the remedy.

263. The effectiveness of the IPT is further underlined by the fact that it can, as a matter of EU law, make an order for reference to the CJEU where an issue arises that is relevant to the dispute before it (see *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service and Secret Intelligence Service*, at paragraph 236 above). The Court has held that the protection of fundamental rights by Community law can be considered to be “equivalent” to that of the Convention system (see *Bosphorus Hava Yolları Turizm ve Ticaret Anonim Şirketi v. Ireland* [GC], no. 45036/98, § 165 ECHR 2005-VI) and it would therefore be surprising if applicants were permitted to bypass a court or tribunal which could have such a significant role in the enforcement of Community law and its fundamental rights guarantees.

264. Insofar as the applicants rely on the fact that the IPT cannot issue a Declaration of Incompatibility (see paragraph 242 above), it is sufficient to note that the Court has not yet accepted that the practice of giving effect to the national courts’ Declarations of Incompatibility by amendment of legislation is “so certain as to indicate that section 4 of the Human Rights Act is to be interpreted as imposing a binding obligation” (see *Burden v. the United Kingdom* [GC], no. 13378/05, § 43, ECHR 2008). Consequently, the relevant question is not whether the IPT can issue a Declaration of Incompatibility, but whether the practice of giving effect to its findings is sufficiently certain.

265. In light of the foregoing considerations, the Court finds that as a general rule the IPT has shown itself to be a remedy, available in theory and practice, which is capable of offering redress to applicants complaining of both specific incidences of surveillance and the general Convention compliance of surveillance regimes. As a result, the complaints made by the applicants in the first and second of the joined cases must be declared inadmissible for non-exhaustion unless they can show that there existed special circumstances absolving them from the requirement to exhaust this remedy.

266. In this regard, they contend that precisely such circumstances existed; namely, that at the time they lodged their applications with this Court they were entitled to rely on *Kennedy* as authority for the proposition that the IPT was not an effective remedy for a complaint about the general Convention compliance of a surveillance regime.

267. Although, at first glance, there would appear to be significant differences between the present case and that of *Kennedy* (for example, as the applicant in *Kennedy* had brought a specific complaint to the IPT the Court was not required to consider the more general complaint entirely in the abstract, and in *Kennedy* the applicant's challenge to the RIPA provisions was a challenge to primary legislation as opposed to the whole legal framework governing the relevant surveillance regime), the Government, for their part, have not sought to distinguish *Kennedy* from the case at hand. Moreover, the case-law of the IPT which the Government have relied on as evidence of its effectiveness as a remedy post-dates the introduction before this Court – on 4 September 2013 and 11 September 2014 – of the complaints made by the applicants in the first and second of the joined cases. For example, the main judgment in the *Liberty* proceedings was delivered on 5 December 2014, the *Belhadj* proceedings concluded on 26 February 2015 and *News Group and Others* was decided on 17 December 2015). While the Court has identified some earlier cases which illustrate the effectiveness of the IPT (for example, *B, A Complaint of Surveillance* and *Paton and Others*), none of these cases concerned a general complaint about the Convention compliance of a surveillance regime. In comparison, the *Liberty* proceedings, *Belhadj* and *News Group and Others* all demonstrate the important and unique role of the IPT in both elucidating the operation of such regimes, and remedying any breaches of the Convention.

268. Consequently, while the Court acknowledges that since *Kennedy* was decided in 2010 the IPT has shown itself to be an effective remedy which applicants complaining about the actions of the intelligence services and/or the general operation of surveillance regimes should first exhaust in order to satisfy the requirements of Article 35 § 1 of the Convention, it would nevertheless accept that at the time the applicants in the first and second of the joined cases introduced their applications, they could not be faulted for relying on *Kennedy* as authority for the proposition that the IPT was not an effective remedy for a complaint about the general Convention compliance of a surveillance regime. It therefore finds that there existed special circumstances absolving these applicants from the requirement that they first bring their complaints to the IPT and, as a consequence, it considers that their complaints cannot be declared inadmissible pursuant to Article 35 § 1 of the Convention.

II. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

269. Cumulatively, the applicants in the three joined cases complain about the Article 8 compatibility of three discrete regimes: the regime for the bulk interception of communications under section 8(4) of RIPA; the intelligence sharing regime; and the regime for the acquisition of

communications data under Chapter II of RIPA. The Court will consider each of these regimes separately.

A. The section 8(4) regime

270. The applicants in all of the joined cases complain that the regime under section 8(4) of RIPA for the bulk interception of communications is incompatible with their right to respect for their rights under Article 8 of the Convention, which reads as follows:

“1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

271. The Government contested that argument. They did not, however, raise any objection under Article 1 of the Convention; nor did they suggest that the interception of communications under the section 8(4) regime was taking place outside the United Kingdom’s territorial jurisdiction. The Court will therefore proceed on the assumption that the matters complained of fall within the jurisdictional competence of the United Kingdom.

1. Admissibility

272. The Court notes that this complaint is not manifestly ill-founded within the meaning of Article 35 § 3 (a) of the Convention. It further notes that it is not inadmissible on any other grounds. It must therefore be declared admissible.

2. Merits

(a) The parties’ submissions

(i) The applicants

273. The applicants accepted that the bulk interception regime had a basis in domestic law. However, they argued that it lacked the quality of law because it was so complex as to be inaccessible to the public and to the Government, reliance was placed on arrangements which were substantially “below the waterline” rather than on clear and binding legal guidelines, and it lacked sufficient guarantees against abuse.

274. In particular, the applicants submitted that the section 8(4) regime did not comply with the six requirements identified by this Court in *Weber and Saravia v. Germany* (dec.), no. 54934/00, ECHR 2006-XI. Firstly, they contended that the purposes for which interception could be permitted (such

as “the interests of national security” and “the economic well-being of the United Kingdom) were too vague to provide a clear limit on the intelligence services’ activities.

275. Secondly, they argued that in practice any person was liable to have his or her communications intercepted under section 8(4). Although the regime was targeted at “external” communications, there was no clear definition of “internal” and “external” communications, and in any event modern technological developments had rendered the distinction between the two meaningless. While the Secretary of State was required to provide descriptions of the material he considered it necessary to examine, the ISC had reported that section 8(4) warrants were framed in generic terms.

276. Thirdly, with regard to the limits on the duration of surveillance, the applicants submitted that, in practice, a section 8(4) warrant could continue indefinitely, being renewed every six months by the Secretary of State pursuant to section 9(1)(b) of RIPA.

277. Fourthly, according to the applicants the procedure for filtering, storing and analysing intercepted material lacked adequate safeguards and gave rise to an unacceptable risk of an arbitrary and disproportionate interference with Article 8 of the Convention. First of all, there was no requirement that the selectors used to filter intercepted communications be identified in the Secretary of State’s certificate accompanying the section 8(4) warrant, and these selectors were not otherwise subject to oversight. Secondly, the section 16 safeguards only applied where a person was “known to be for the time being in the British Islands”. Thirdly, the protections in section 16 of RIPA only applied to the “content” of intercepted communications, and not the filtering, storage and analysis of “related communications data”, despite the fact that communications data was capable of providing the Government with a detailed profile of the most intimate aspects of a person’s private life.

278. Fifthly, in relation to the communication of intercepted material, the applicants contended that the requirement that the Secretary of State ensure that its disclosure was limited to “the minimum that is necessary for the authorised purposes” was an ineffective safeguard. The authorised purposes enumerated in section 15(4) of RIPA were extremely wide, and included situations where the information was or was “likely to become” necessary for any of the purposes specified in section 5(3) of RIPA.

279. Sixth and finally, the applicants submitted that there were no effective or binding safeguards against the disproportionate retention of intercepted data. Indeed, according to the applicants it was clear from the third IPT judgment in the *Liberty* proceedings that Amnesty International’s communications had been stored without the appropriate (automated) deletion procedures being followed, and neither the intelligence services nor the oversight and audit mechanisms had detected this.

280. In addition to arguing that the *Weber* requirements were not satisfied, the applicants in any event contended that they were no longer sufficient to ensure that a communications surveillance regime was compatible with Article 8 of the Convention. *Weber* had been decided in 2006, and subsequent technological developments meant that Governments could now create detailed and intrusive profiles of intimate aspects of private lives by analysing patterns of communications on a bulk basis. The applicants therefore identified a number of additional requirements which they believed were now necessary to ensure the Convention compliance of a legal framework for surveillance: the requirement for objective evidence of reasonable suspicion in relation to the persons for whom data was being sought; prior independent judicial authorisation of interception warrants; and the subsequent notification of the surveillance subject.

281. Finally, the applicants submitted that the section 8(4) regime was disproportionate. In their view the intelligence services were systematically collecting both content and communications data on a massive scale and retaining it for future searching and use. Such a blanket approach fell foul of the principles established in *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, ECHR 2008 and *M.K. v. France*, no. 19522/09, 18 April 2013.

(ii) *The Government*

282. At the outset, the Government submitted that the information and intelligence obtained under the section 8(4) regime was critical to the protection of the United Kingdom from national security threats; in particular, but not exclusively, from the threat of terrorism. This was especially so given the current level of sophistication of terrorists and criminals in communicating over the Internet in ways that avoided detection, whether through the use of encryption, the adoption of bespoke communications systems, or simply because of the volume of Internet traffic in which they could now hide their communications. Imposing additional fetters on the interception of communications would damage the State's ability to safeguard national security and combat serious crime at exactly the point when advances in communication technology had increased the threat from terrorists and criminals using the Internet.

283. The seriousness of the terrorist threat was underscored by a number of recent attacks across the United Kingdom and Europe, including the attack on Westminster Bridge on 22 March 2017, the Manchester Arena bombing of 22 May 2017, the attack on London Bridge on 3 June 2017, the attacks in Barcelona and Cambrils on 17 August 2017, and the attack on the London Underground on 15 September 2017. The Government therefore submitted that under the Convention scheme, it was properly for States to judge what was necessary to protect the general community from such threats. While those systems were subject to the Court's scrutiny, it had

consistently – and rightly – afforded States a broad margin of appreciation in this field so as not to undermine the effectiveness of systems for obtaining life-saving intelligence that could not be gathered any other way.

284. Although the Government denied that the section 8(4) regime permitted mass surveillance or generalised access to communications, it accepted that it permitted, pursuant to the lawful authority of warrants, the bulk interception of bearers for wanted external communications. In the Government's opinion, the distinction between "internal" and "external" communications was sufficiently clear, and in any event it operated primarily as a safeguard at the macro level; that is, in determining which bearers should be targeted for interception. The Government further contended that bulk interception was critical for the discovery of threats and hitherto unknown targets which might be responsible for threats. Even when the identity of targets was known, they were likely to use a variety of different means of communication, and change those means frequently. Electronic communications did not traverse the Internet by routes that could necessarily be predicted; rather, they took the most efficient route, determined by factors such as cost and the volume of traffic passing over particular parts of the Internet at different times of the day. In addition, communications sent over the Internet were broken down into small pieces (or "packets"), which were transmitted separately, often through different routes. In the opinion of the Government, it was therefore necessary to intercept all communications travelling over more than one bearer to maximise the chance of identifying and obtaining the communications being sent to known targets.

285. With regard to whether the interference complained of was "in accordance with the law", the Government relied on the fact that it had its basis in primary legislation, namely section 8(4) of RIPA, supplemented by the Interception of Communications Code of Practice ("the IC Code"). It had been further clarified by the reports of the Interception of Communications Commissioner, which were also public documents.

286. In relation to the *Weber* requirements the Government argued that the first foreseeability requirement, being the "offences" which might give rise to an interception order, was satisfied by section 5 of RIPA, which defined the purposes for which the Secretary of State could issue an interception warrant. In *Kennedy*, despite the applicant's criticism of the terms "national security" and "serious crime", the Court had found the description of the offences which might give rise to an interception order to be sufficiently clear (*Kennedy*, cited above, § 159).

287. Relying on *Weber*, the Government submitted that the second foreseeability requirement (the categories of people liable to have their communications intercepted) applied at both the interception stage and the selection stage. As regards the interception stage, a section 8(4) warrant was targeted at "external" communications, although in principle it might

authorise the interception of “internal” communications insofar as that was necessary in order to intercept the external communications to which the warrant related. With regard to the selection stage, section 16(1) of RIPA provided that no intercepted material could be read, looked at or listened to by any person unless it fell within the Secretary of State’s certificate, and it was proportionate in the circumstances to do so. Furthermore, section 16(2) placed sufficiently precise limits on the extent to which intercepted material could be selected to be read, looked at or listened to according to a factor which was referable to an individual known to be for the time being in the British Islands and which had as (one of) its purpose(s) the identification of material contained in communications sent by or intended for him.

288. The Government further argued that paragraphs 6.22-6.24 of the IC Code made sufficient provision for the duration and renewal of a section 8(4) warrant, thereby complying with the third requirement identified in *Weber*. Pursuant to section 9(2) of RIPA, a section 8(4) warrant could only be renewed if the Secretary of State believed that it continued to be necessary, and if the Secretary of State believed that the warrant was no longer necessary, section 9(3) of RIPA required that it be cancelled.

289. According to the Government, insofar as intercepted material could not be read, looked at or listened to by a person pursuant to section 16 of RIPA, it could not be used at all. Prior to its destruction, paragraph 7.7 of the IC Code required that it be stored securely. For material that could be read, looked at and listened to pursuant to section 16, the Government submitted that the regime satisfied the fourth of the *Weber* requirements. In particular, material had to be selected for examination through the application of search terms by equipment operating automatically for that purpose. If an analyst then wished to select material for examination, paragraphs 7.14-7.16 of the IC Code required that he or she create a record setting out why access was required and proportionate, consistent with the applicable certificate, and stating any circumstances likely to give rise to a degree of collateral infringement of privacy, and any measures taken to reduce the extent of that infringement. That record had to be retained for the purpose of subsequent audit. Paragraphs 7.11-7.20 further required that material should only be read, looked at or listened to by authorised persons receiving regular training in the operation of section 16 of RIPA and the requirements of necessity and proportionality. Finally, material could only be used by the intelligence services in accordance with their statutory functions, and only insofar as was proportionate under section 6(1) of the Human Rights Act 1998.

290. The Government further submitted that the section 8(4) regime satisfied the fifth *Weber* requirement. Section 15(2) set out the precautions to be taken when communicating intercepted material to other people. These precautions served to ensure that only so much intercepted material as was “necessary” for the authorised purpose could be disclosed. Paragraphs 7.4

and 7.5 of the IC Code further provided that where intercepted material was to be disclosed to a foreign State, the intelligence services had to take reasonable steps to ensure that the authorities of that State had and would maintain the necessary procedures to safeguard the intercepted material, and to ensure that it was disclosed, copied, distributed and retained only to the minimum extent necessary. It could only be further disclosed to the authorities of a third country if explicitly agreed. Finally, any disclosure would have to satisfy the constraints imposed by sections 1-2 of the Security Services Act 1989, sections 1-4 of the Intelligence Services Act 1994 as read with section 19(3)-(5) of the Counter Terrorism Act 2008 and section 6(1) of the Human Rights Act 1998.

291. With regard to the final *Weber* requirement, the Government contended that section 15(3) of RIPA and paragraphs 7.8-7.9 of the IC Code made sufficient provision for the circumstances in which intercepted material had to be erased or destroyed (including the obligation to review retention at appropriate intervals, and the specification of maximum retention periods which should normally be no longer than two years).

292. Although the Government acknowledged that the safeguards in section 16 of RIPA did not apply to “related communications data”, they argued that the covert acquisition of related communications data was less intrusive than the covert acquisition of content and, as such, the Court had never applied the *Weber* requirements to powers to acquire communications data. It was therefore their contention that instead of the list of six specific foreseeability requirements, the test in respect of communications data should be the more general one of whether the law indicated the scope of any discretion and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.

293. According to the Government, the section 8(4) regime satisfied this test as regards the obtaining and use of related communications data. First of all, “related communications data” as defined in sections 20 and 21 of RIPA was not synonymous with “metadata” but was instead a limited subset of metadata. Secondly, the section 8(4) regime was sufficiently clear as to the circumstances in which the intelligence services could obtain related communications data (namely, by the interception of bearers pursuant to a section 8(4) warrant). Once obtained, access to related communications data had to be necessary and proportionate under section 6(1) of the Human Rights Act 1998 and subject to the constraints in sections 1-2 of the Security Services Act and sections 1-4 of the Intelligence Services Act. Storage, handling, use and disclosure of related communications data, including access by a foreign intelligence partner, would be constrained by section 15 of RIPA and paragraphs 7.1-7.10 of the IC Code. Finally, the Government argued that there was good reason for exempting related communications data from the safeguards in section 16; in order for section 16 to work, the

intelligence services needed to be able to assess whether a potential target was “for the time being in the British Islands”.

294. Finally, the Government addressed the applicants’ proposals for “updating” the *Weber* requirements. They submitted that any requirement of “reasonable suspicion” would largely preclude the operation of bulk interception regimes, despite the fact that the Court had permitted such monitoring in *Weber*. Furthermore, in *Kennedy* (cited above, § 167) the Court clearly held that judicial authorisation could be either *ex ante* or *post facto*. In that case the Court had found that the oversight provided by the Commissioner, the ISC and the IPT had compensated for any lack of prior judicial authorisation. Finally, any requirement to notify a suspect of the use of bulk data tools against him could fundamentally undermine the work of the intelligence services and potentially threaten the lives of covert human intelligence sources close to the suspect. It would also be wholly impractical in the section 8(4) context, since many of the targets would be overseas and their personal details might be unknown or imperfectly known.

(b) The submissions of the third parties

(i) Article 19

295. Article 19 submitted that mass interception powers were by their very nature inherently incapable of being exercised in a proportionate manner and, as such, were inherently incompatible with the requirements of the Convention. Article 19 therefore urged the Court to conclude that only targeted surveillance based on reasonable suspicion and authorised by a judge constituted a legitimate restriction on the right to privacy.

(ii) Access Now

296. Access Now submitted that the mass surveillance at issue in the present case failed to comply with the International Covenant on Civil and Political Rights (“ICCPR”) and the International Principles on the Application of Human Rights to Communications Surveillance since the United Kingdom had not demonstrated that such surveillance was strictly necessary or proportionate. They further contended that surveillance programmes should not be considered independently but should instead be viewed in relation to the entirety of a nation’s surveillance activities as machine learning, through which mathematical algorithms could draw inferences from collections of data, had increased the invasiveness of big data sets and data mining.

(iii) ENNHRI

297. The ENNHRI also drew the Court’s attention to international instruments such as the ICCPR, the American Convention on Human Rights, and the EU Charter of Fundamental Rights. It observed that in 2015

the Human Rights Committee reviewed the State Party report of the United Kingdom of Great Britain and Northern Ireland. It expressed concern that RIPA provided for untargeted warrants for the interception of external communications without affording the same safeguards as applied to internal communications, and it made a number of detailed recommendations, including the creation of sufficiently precise and foreseeable legal provisions, and judicial involvement in the authorisation of such measures.

(iv) *The Helsinki Foundation for Human Rights (“HFHR”)*

298. The HFHR described their experience challenging the surveillance of communications by public authorities in Poland, which culminated in the Constitutional Tribunal finding certain aspects of the relevant legislation to be unconstitutional. The legislation was subsequently amended.

(v) *The International Commission of Jurists (“ICJ”)*

299. The ICJ submitted that in light of the scale and scope of the interference with privacy entailed in mass surveillance, the distinction between the acquisition of metadata and content had become out-dated. Furthermore, the fact that, in a mass surveillance operation, elements of the interference with rights might take place outside a State’s territorial jurisdiction didn’t preclude that State’s responsibility, since its control over the information was sufficient to establish jurisdiction.

(vi) *Open Society Justice Initiative (“OSJI”)*

300. OSJI submitted that both the amount of data available for interception today and governments’ appetite for data far exceeded what was possible in the past. Consequently, bulk interception was a particularly serious interference with privacy which could, through its “chilling effect”, potentially interfere with other rights such as freedom of expression and freedom of association. To be lawful, bulk interception should therefore satisfy several preconditions: the governing law had to be sufficiently precise; the scope of the information gathered had to be limited by time and geography; and information should only be gathered based on “reasonable suspicion”.

(vii) *European Digital Rights (“EDRi”) and other organisations active in the field of human rights in the information society*

301. EDRi and others argued that the present case offered the Court a crucial opportunity to revise its framework for the protection of metadata. Governments had built their surveillance programmes based on the distinction drawn between content and metadata in *Malone v. the United Kingdom*, 2 August 1984, Series A no. 82, but at the time that case was decided neither the Internet nor mobile phones existed. Today, metadata

could paint a detailed and intimate picture of a person: it allowed for mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with. Moreover, the level of detail that could be gleaned was magnified when analysed on a large scale. Indeed, Stewart Baker, general counsel of the NSA, had indicated that metadata could disclose everything about someone's life, and that if you had enough metadata, you wouldn't need content. As a result, different degrees of protection should not be afforded to personal data based on the arbitrary and irrelevant distinction between content and metadata, but rather on the inferences that could be drawn from the data.

(viii) The Law Society of England and Wales

302. The Law Society expressed deep concern about the implications of the section 8(4) regime for the principle of legal professional privilege. In particular, the regime permitted the interception of legally privileged and confidential communications between lawyers and clients, even when both were in the United Kingdom. It also permitted the routine collection of metadata attaching to such communications. Furthermore, once intercepted these legally privileged communications could be used, provided that the primary purpose and object of the warrant was the collection of external communications. This arrangement – and the absence of adequate constraints on the use of such material – was apt to have a potentially severe chilling effect on the frankness and openness of lawyer-client communications.

(c) The Court's assessment

(i) General principles relating to secret measures of surveillance, including the interception of communications

303. Although the Court has developed extensive jurisprudence on secret measures of surveillance, its case-law concerns many different forms of surveillance, including, but not limited to, the interception of communications. It also concerns many different forms of “interference” with applicants' right to respect for their private lives; for example, while some cases concern the interception of the content of communications, others concern the interception or obtaining of communications data, or the tracking of individuals via GPS. As the Court has at times differentiated between the different types of surveillance and the different forms of interference, there is no one set of general principles which apply in all cases concerning secret measures of surveillance. The following principles can, however, be extrapolated from the Court's case-law.

304. Any interference with an individual's Article 8 rights can only be justified under Article 8 § 2 if it is in accordance with the law, pursues one

or more of the legitimate aims to which that paragraph refers and is necessary in a democratic society in order to achieve any such aim (see *Roman Zakharov*, cited above, § 227, and *Kennedy*, cited above, § 130).

305. According to the Court's well established case-law, the wording "in accordance with the law" requires the impugned measure to have some basis in domestic law (as opposed to a practice which does not have a specific legal basis – see *Heglas v. the Czech Republic*, no. 5935/02, § 74, 1 March 2007). It must also be compatible with the rule of law, which is expressly mentioned in the Preamble to the Convention and inherent in the object and purpose of Article 8. The law must therefore be accessible to the person concerned and foreseeable as to its effects (see *Roman Zakharov*, cited above, § 228; see also, among many other authorities, *Rotaru v. Romania* [GC], no. 28341/95, § 52, ECHR 2000-V; *S. and Marper*, cited above, § 95, and *Kennedy*, cited above, § 151).

306. The Court has held on several occasions that the reference to "foreseeability" in the context of secret surveillance cannot be the same as in many other fields. Foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to resort to such measures so that he can adapt his conduct accordingly. However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on secret surveillance measures, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures (see *Roman Zakharov*, cited above, § 229; see also *Malone*, cited above, § 67, *Leander*, cited above, § 51; *Huvig v. France*, 24 April 1990, § 29, Series A no. 176-B; *Valenzuela Contreras v. Spain*, 30 July 1998, § 46, Reports of Judgments and Decisions 1998-V; *Rotaru*, cited above, § 55; *Weber and Saravia*, cited above, § 93; *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, § 75, 28 June 2007). Moreover, the law must indicate the scope of any discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (see *Roman Zakharov*, cited above, § 230; see also, among other authorities, *Malone*, cited above, § 68; *Leander*, cited above, § 51; *Huvig*, cited above, § 29; and *Weber and Saravia*, cited above, § 94).

307. In its case-law on the interception of communications in criminal investigations, the Court has developed the following minimum requirements that should be set out in law in order to avoid abuses of power: the nature of offences which may give rise to an interception order; a

definition of the categories of people liable to have their communications intercepted; a limit on the duration of interception; 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 intercepted data may or must be erased or destroyed (see *Huvig*, cited above, § 34; *Valenzuela Contreras*, cited above, § 46; *Weber and Saravia*, cited above, § 95; and *Association for European Integration and Human Rights and Ekimdzhiiev*, cited above, § 76). In *Roman Zakharov* (cited above, § 231) the Court confirmed that the same six minimum requirements also applied in cases where the interception was for reasons of national security; however, in determining whether the impugned legislation was in breach of Article 8, it also had regard to the arrangements for supervising the implementation of secret surveillance measures, any notification mechanisms and the remedies provided for by national law (*Roman Zakharov*, cited above, § 238).

308. As to the question whether an interference was “necessary in a democratic society” in pursuit of a legitimate aim, the Court has acknowledged that, when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant’s right to respect for his or her private life, the national authorities enjoy a certain margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security. However, this margin is subject to European supervision embracing both legislation and decisions applying it. In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse. The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the 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. The Court has to determine whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the “interference” to what is “necessary in a democratic society” (see *Roman Zakharov*, cited above, § 232; see also *Klass and Others v. Germany*, 6 September 1978, §§ 49, 50 and 59, Series A no. 28, *Weber and Saravia*, cited above, § 106 and *Kennedy*, cited above, §§ 153 and 154).

309. Review and supervision of secret surveillance measures may come into play at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual’s knowledge. Consequently, since the individual will

necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights. In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure (see *Roman Zakharov*, cited above, § 233; see also *Klass and Others*, cited above, §§ 55 and 56).

310. As regards the third stage, after the surveillance has been terminated, the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers. There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively (see *Roman Zakharov*, cited above, § 234; see also *Klass and Others*, cited above, § 57, and *Weber and Saravia*, cited above, § 135) or, in the alternative, unless any person who suspects that he or she has been subject to surveillance can apply to courts, whose jurisdiction does not depend on notification to the surveillance subject of the measures taken (see *Roman Zakharov*, cited above, § 234; see also *Kennedy*, cited above, § 167).

(ii) *Existing case-law on the bulk interception of communications*

311. The Court has considered the Convention compatibility of regimes which expressly permit the bulk interception of communications on two occasions: first in *Weber and Saravia* (cited above), and then in *Liberty and Others v. the United Kingdom*, no. 58243/00, 1 July 2008.

312. In *Weber and Saravia* the applicants complained about the process of strategic monitoring under the amended G10 Act, which authorised the monitoring of international wireless telecommunications. Signals emitted from foreign countries were monitored by interception sites situated on German soil with the aid of certain catchwords which were listed in the monitoring order. Only communications containing these catchwords were recorded and used. Having particular regard to the six “minimum requirements” set out in paragraph 307 above, the Court considered that there existed adequate and effective guarantees against abuses of the State’s strategic monitoring powers. It therefore declared the applicants’ Article 8 complaints to be manifestly ill-founded.

313. In *Liberty and Others* the Court was considering the regime under section 3(2) of the Interception of Communications Act 1985, which was in effect the predecessor of the regime under section 8(4) of RIPA.

Section 3(2) allowed the executive to intercept communications passing between the United Kingdom and an external receiver. At the time of issuing a section 3(2) warrant, the Secretary of State was required to issue a certificate containing a description of the intercepted material which he considered should be examined. The 1985 Act provided that material could be contained in a certificate, and thus listened to or read, if the Secretary of State considered that this was required in the interests of national security, the prevention of serious crime or the protection of the United Kingdom's economy. However, external communications emanating from a particular address in the United Kingdom could only be included in a certificate for examination if the Secretary of State considered it necessary for the prevention or detection of acts of terrorism. The Court held that the domestic law at the relevant time (which predated the adoption of the Interception of Communications Code of Practice – see, in particular, paragraph 109 above) did not indicate with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications. In particular, it did not set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material.

(iii) *The test to be applied in the present case*

314. The Court has expressly recognised that the national authorities enjoy a wide margin of appreciation in choosing how best to achieve the legitimate aim of protecting national security (see *Weber and Saravia*, cited above, § 106). Furthermore, in *Weber and Saravia* and *Liberty and Others* the Court accepted that bulk interception regimes did not *per se* fall outside this margin. Although both of these cases are now more than ten years old, given the reasoning of the Court in those judgments and in view of the current threats facing many Contracting States (including the scourge of global terrorism and other serious crime, such as drug trafficking, human trafficking, the sexual exploitation of children and cybercrime), advancements in technology which have made it easier for terrorists and criminals to evade detection on the Internet, and the unpredictability of the routes via which electronic communications are transmitted, the Court considers that the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security is one which continues to fall within States' margin of appreciation.

315. Nevertheless, as indicated previously, it is evident from the Court's case-law over several decades that all interception regimes (both bulk and targeted) have the potential to be abused, especially where the true breadth of the authorities' discretion to intercept cannot be discerned from the relevant legislation (see, for example, *Roman Zakharov*, cited above, and

Szabó and Vissy v. Hungary, no. 37138/14, 12 January 2016). Therefore, while States enjoy a wide margin of appreciation in deciding what type of interception regime is necessary to protect national security, the discretion afforded to them in operating an interception regime must necessarily be narrower. In this regard, the Court has identified six minimum requirements that both bulk interception and other interception regimes must satisfy in order to be sufficiently foreseeable to minimise the risk of abuses of power (see paragraph 307 above).

316. The applicants argue that in the present case the Court should “update” those requirements by including requirements for objective evidence of reasonable suspicion in relation to the persons for whom data is being sought, prior independent judicial authorisation of interception warrants, and the subsequent notification of the surveillance subject (see paragraph 280 above). In their view, such changes would reflect the fact that due to recent technological developments the interception of communications now has greater potential than ever before to paint an intimate and detailed portrait of a person’s private life and behaviour. However, while the Court does not doubt the impact of modern technology on the intrusiveness of interception, and has indeed emphasised this point in its case-law, it would be wrong automatically to assume that bulk interception constitutes a greater intrusion into the private life of an individual than targeted interception, which by its very nature is more likely to result in the acquisition and examination of a large volume of his or her communications. In any event, although the Court would agree that the additional requirements proposed by the applicants might constitute important safeguards in some cases, for the reasons set out below it does not consider it appropriate to add them to the list of minimum requirements in the case at hand.

317. First of all, requiring objective evidence of reasonable suspicion in relation to the persons for whom data is being sought and the subsequent notification of the surveillance subject would be inconsistent with the Court’s acknowledgment that the operation of a bulk interception regime in principle falls within a State’s margin of appreciation. Bulk interception is by definition untargeted, and to require “reasonable suspicion” would render the operation of such a scheme impossible. Similarly, the requirement of “subsequent notification” assumes the existence of clearly defined surveillance targets, which is simply not the case in a bulk interception regime.

318. Judicial authorisation, by contrast, is not inherently incompatible with the effective functioning of bulk interception. Nevertheless, as the Venice Commission acknowledged in their report on the Democratic Oversight of Signals Intelligence Agencies (see paragraph 212 above), while the Court has recognised that judicial authorisation is an “important safeguard against arbitrariness” (see *Roman Zakharov*, cited above, § 249),

to date it has not considered it to be a “necessary requirement” or the exclusion of judicial control to be outside “the limits of what may be deemed necessary in a democratic society” (see, for example, *Roman Zakharov*, cited above, § 258; see also *Klass and Others*, cited above, §§ 51 and 56; *Weber and Saravia*, cited above, § 115; *Kennedy*, cited above, § 167; and *Szabó and Vissy*, cited above, § 77). There would appear to be good reason for this. The Court has found it “desirable to entrust supervisory jurisdiction to a judge” because, as a result of the secret nature of the surveillance, the individual will usually be unable to seek a remedy of his or her own accord (see *Roman Zakharov*, cited above, § 233). However, that is not the case in every contracting State. In the United Kingdom, for example, any person who thinks that he or she has been subject to secret surveillance can lodge a complaint with the IPT (see paragraph 250 above). Consequently, in *Kennedy* the Court accepted that regardless of the absence of prior judicial authorisation, the existence of independent oversight by the IPT and the Interception of Communications Commissioner provided adequate safeguards against abuse (see *Kennedy*, cited above, §§ 167-169). In this regard, the Venice Commission also noted that independent oversight may be able to compensate for an absence of judicial authorisation (see paragraph 212 above).

319. Secondly, the Court has acknowledged that “the possibility of improper action by a dishonest, negligent or over-zealous official can never be completely ruled out whatever the system” (see *Klass and Others*, cited above, § 59), and one need only look at its most recent jurisprudence to find examples of cases where prior judicial authorisation provided limited or no protection against abuse. For example, in *Roman Zakharov*, any interception of communications had to be authorised by a court and the judge had to give reasons for the decision to authorise interceptions. However, as judicial scrutiny was limited in scope and the police had the technical means to circumvent the authorisation procedure and to intercept any communications without obtaining prior judicial authorisation, the Court found that Russian law was incapable of keeping the “interference” to what was “necessary in a democratic society”. Similarly, in *Association for European Integration and Human Rights and Ekimdzhiiev* the relevant law required judicial authorisation before interception could take place. Nevertheless, the Court found that numerous abuses had taken place (according to a recent report, more than 10,000 warrants were issued over a period of some twenty-four months). More recently, in *Mustafa Sezgin Tanrikulu v. Turkey*, no. 27473/06, § 64, 18 July 2017 the Court found a violation of Article 8 where an assize court had granted the National Intelligence Agency permission to intercept all domestic and international communications for a month and a half with a view to identifying terrorist suspects.

320. Therefore, while the Court considers judicial authorisation to be an important safeguard, and perhaps even “best practice”, by itself it can neither be necessary nor sufficient to ensure compliance with Article 8 of the Convention (see *Klass and Others*, cited above, § 56). Rather, regard must be had to the actual operation of the system of interception, including the checks and balances on the exercise of power, and the existence or absence of any evidence of actual abuse (see *Association for European Integration and Human Rights and Ekimdzhev*, cited above, § 92). Accordingly, the Court will examine the justification for any interference in the present case by reference to the six minimum requirements, adapting them where necessary to reflect the operation of a bulk interception regime. It will also have regard to the additional relevant factors which it identified in *Roman Zakharov*, but did not classify as “minimum requirements”; namely, the arrangements for supervising the implementation of secret surveillance measures, any notification mechanisms and the remedies provided for by national law (see paragraph 307 above).

(α) The existence of an interference

321. The Government do not dispute that there has been an interference with the applicants’ Article 8 rights.

(β) Justification for the interference

322. As already noted, an interference can only be justified under Article 8 § 2 if it is in accordance with the law, pursues one or more legitimate aims and is necessary in a democratic society in order to achieve any such aim (see paragraph 303 above). In cases where the legislation permitting secret surveillance is contested before the Court, the lawfulness of the interference is closely related to the question whether the “necessity” test has been complied with and it is therefore appropriate for the Court to address jointly the “in accordance with the law” and “necessity” requirements (see *Roman Zakharov*, cited above, § 236 and *Kennedy*, cited above, § 155). The “quality of law” in this sense implies that the domestic law must not only be accessible and foreseeable in its application, but it must also ensure that secret surveillance measures are applied only when “necessary in a democratic society”, in particular by providing for adequate and effective safeguards and guarantees against abuse.

323. The parties do not dispute that the section 8(4) regime had a basis in domestic law; nor do they dispute that the regime pursued the legitimate aims of the protection of national security, the prevention of crime and the protection of the economic well-being of the country. The applicants do, however, contest the quality of domestic law and, in particular, its accessibility and foreseeability.

324. The Court will therefore assess in turn the accessibility of the domestic law, followed by its foreseeability and necessity, having regard to

the six minimum requirements established in its case law, before turning its attention to the arrangements for supervising the implementation of secret surveillance measures, any notification mechanisms and the remedies provided for by national law (see paragraph 307 above).

- *Accessibility*

325. The applicants challenge the accessibility of domestic law on the grounds that it is too complex to be accessible to the public, and it relies on “below the waterline” arrangements. It is true that most of the reports into the United Kingdom’s secret surveillance regimes have criticised the piecemeal development – and subsequent lack of clarity – of the legal framework (see paragraphs 152, 162 and 167 above). However, as with other cases in which domestic law has been considered *in abstracto* and amendments have been made to the legislation while the application was pending (see, for example, *Association for European Integration and Human Rights and Ekimdzhiev*), in the present case the Court must review the Convention compliance of the law in force at the date of its examination of the applicants’ complaints. It therefore can, and should, take into account the IC Code which was amended in 2016 to clarify the legal framework and reflect the further disclosures which were made following the Snowden revelations and which are examined in detail in the ISC report, the Anderson report and the ISR report (see paragraphs 90, 148-150, 160-165 and 166-172 above). As the IC Code is a public document, subject to the approval of both Houses of Parliament, and has to be taken into account both by those exercising interception duties and by courts and tribunals, the Court has expressly accepted that its provisions could be taken into consideration in assessing the foreseeability of the RIPA regime (see *Kennedy*, cited above, § 157).

326. Insofar as the applicants complain about the existence of “below the waterline” arrangements, the Court has acknowledged that States do not have to make public all the details of the operation of a secret surveillance regime, provided that sufficient information is available in the public domain (see *Roman Zakharov*, cited above, §§ 243-244 and 247; see also, among many examples, *Szabó and Vissy*, cited above, § 64, and *Kennedy*, cited above, § 159). In the context of secret surveillance, it is inevitable that “below the waterline” arrangements will exist, and the real question for the Court is whether it can be satisfied, based on the “above the waterline” material, that the law is sufficiently foreseeable to minimise the risk of abuses of power. This is a question that goes to the foreseeability and necessity of the relevant law, rather than its accessibility.

327. Therefore, while the Court concurs with several of the aforementioned domestic reports that RIPA and the accompanying surveillance framework are extremely complex, in the present case it will concentrate on the requirements of “foreseeability” and “necessity”.

- *The scope of application of secret surveillance measures*

328. The first two minimum requirements have traditionally been referred to as the nature of the offences which might give rise to an interception order and a definition of the categories of people liable to have their telephones tapped. In *Roman Zakharov* the Court made clear that pursuant to these two requirements “the national law must define the scope of application of secret surveillance measures by giving citizens an adequate indication as to the circumstances in which public authorities are empowered to resort to such measures” (see *Roman Zakharov*, cited above, §§ 243).

329. In a targeted interception regime, the nature of the communications to be intercepted should be tightly defined, but once interception takes place it is likely that all – or nearly all – of the intercepted communications are analysed. The opposite will normally be true of a bulk interception regime, where the discretion to intercept is broader, but stricter controls will be applied at the selection for examination stage. In fact, in the present case, it is clear from Chapter 6 of the IC Code (see paragraph 90 above), the ISC report (see paragraphs 151-159 above), the first IPT judgment in the *Liberty* proceedings (see paragraphs 41-49 above) and the Government’s observations that there are four distinct stages to the section 8(4) regime:

1. The interception of a small percentage of Internet bearers, selected as being those most likely to carry external communications of intelligence value.
2. The filtering and automatic discarding (in near real-time) of a significant percentage of intercepted communications, being the traffic least likely to be of intelligence value.
3. The application of simple and complex search criteria (by computer) to the remaining communications, with those that match the relevant selectors being retained and those that do not being discarded.
4. The examination of some (if not all) of the retained material by an analyst).

330. Thus, in addressing the first two minimum requirements, the Court will examine first, whether the grounds upon which a warrant can be issued are sufficiently clear; secondly, whether domestic law gives citizens an adequate indication of the circumstances in which their communications might be intercepted; and thirdly, whether domestic law gives citizens an adequate indication of the circumstances in which their communications might be selected for examination (see paragraph 328 above).

331. According to RIPA and the IC Code, the Secretary of State can only issue a warrant if he is satisfied that it is necessary in the 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 so far as those interests are also relevant to the interests of national security; and that the conduct authorised by the warrant is

proportionate to what is sought to be achieved by that conduct. Pursuant to domestic law, when assessing necessity and proportionality, account should be taken of whether the information sought under the warrant could reasonably be obtained by other means (section 5(3) of RIPA and Chapter 6 of the IC Code – see paragraphs 57 and 90 above). It is clear that insofar as RIPA and the IC Code use the terms “necessity” and “proportionality” they are intended to ensure compliance with the requirements of Articles 8 and 10 of the Convention and should therefore be understood in the Convention sense (see paragraph 3.5 of the IC Code, at paragraph 90 above).

332. The Court has held that the condition of foreseeability does not require States to set out exhaustively by name the specific offences which may give rise to interception, provided that there is sufficient detail about the nature of the offences in question (see *Roman Zakharov*, cited above, §§ 243-244; see also, among many examples, *Szabó and Vissy*, cited above, § 64, and *Kennedy*, cited above, § 159). Moreover, the Court has expressly recognised the need to avoid excessive rigidity in the wording of certain statutes and to keep pace with changing circumstances (see *Szabó and Vissy*, cited above, § 64 and *Kokkinakis v. Greece*, 25 May 1993, § 40, Series A no. 260-A).

333. In *Kennedy* the Court had to consider whether the section 5(3) grounds (which apply to both section 8(1) and section 8(4) warrants) provided sufficient detail about the nature of the offences that might give rise to an interception order. It found that the term “national security” was frequently employed in both national and international legislation and constituted one of the legitimate aims to which Article 8 § 2 referred. It further noted that threats to national security tended to vary in character and might be unanticipated or difficult to define in advance. Finally, the Interception of Communications Commissioner had clarified that in practice “national security” allowed surveillance of activities which threatened the safety or well-being of the State and activities which were intended to undermine or overthrow Parliamentary democracy by political, industrial or violent means. It therefore found the term to be sufficiently clear (see *Kennedy*, cited above, § 159).

334. Furthermore, the Court observes that “serious crime” is clearly defined in section 81 of RIPA (see paragraphs 58-59 above; see also *Kennedy*, cited above, § 159) and the IC Code has clarified that the purpose of safeguarding the economic well-being of the United Kingdom is restricted to those interests which are also relevant to the interests of national security (see paragraph 90 above).

335. The Court therefore considers that section 5(3) is sufficiently clear, giving citizens an adequate indication of the circumstances in which and the conditions on which a section 8(4) warrant might be issued.

336. As for the persons liable to have their communications intercepted, it is clear that this category is wide. Section 8(4) only permits the Secretary

of State to issue a warrant for the interception of external communications, which in principle excludes communications where both of the parties are in the British Islands. Although there has been some confusion about the application of the terms “external communications” and “internal communications” to modern forms of communications, the Secretary of State for the Foreign and Commonwealth, in giving evidence to the Intelligence and Security Committee of Parliament in October 2014, provided clarification about the status of emails, web-browsing, social media and cloud storage (see paragraph 71 above). However, even where it is clear that a communication is “internal”, as it is between two people in the British Islands, in practice, some or all of its parts might be routed through one or more other countries, and would therefore be at risk of being intercepted under the section 8(4) regime. This is expressly permitted by section 5(6) of RIPA, which allows the interception of communications not identified in the warrant (see paragraph 63 above).

337. That being said, it is clear that the targeted bearers are not chosen at random. They are selected because they are believed to be the most likely to carry external communications of intelligence interest (paragraph 6.7 of the IC Code, at paragraph 90 above and the Annual Report of the Interception of Communications Commissioner for 2016, at paragraph 178 above). Therefore, while anyone could potentially have their communications intercepted under the section 8(4) regime, it is clear that the intelligence services are neither intercepting everyone’s communications, nor exercising an unfettered discretion to intercept whatever communications they wish. In practice, one of the grounds set out in section 5(3) of RIPA must be satisfied, bulk interception must be proportionate to the aim sought to be achieved, and – at least at the macro level of selecting the bearers for interception – only external communications can be targeted.

338. As the ISC observed, it would be desirable for the criteria for selecting the bearers to be subject to greater oversight by the Commissioner (see paragraph 157 above). However, the Court has already noted that by its very nature a bulk interception regime will allow the authorities a broad discretion to intercept communications and, as such, it does not consider this fact alone to be fatal to the Article 8 compliance of the section 8(4) regime. While the discretion to intercept should not be unfettered – since the interception and filtering of a communication, even if it is subsequently discarded in near real-time, is sufficient to constitute an interference with a persons’ rights under Article 8 of the Convention –, more rigorous safeguards will be required at the third and fourth stages identified in paragraph 329 above, as any interference in such cases will be significantly greater.

339. With regard to the selection of communications for examination, once communications are intercepted and filtered, those not discarded in near real-time are further searched; in the first instance by the automatic

application, by computer, of simple selectors (such as email addresses or telephone numbers) and initial search criteria, and subsequently by the use of complex searches (see paragraph 6.4 of the IC Code at paragraph 90; see also the ISC report at paragraphs 151-159 above and the Government's observations in the present case). In *Liberty and Others*, the Court compared the predecessor of the section 8(4) regime unfavourably with the German system under consideration in *Weber and Saravia*, noting that the G10 Act authorised the Federal Intelligence Service to carry out monitoring of communications only with the aid of search terms which served, and were suitable for, the investigation of the dangers described in the monitoring order and which search terms had to be listed in the monitoring order (*Liberty and Others*, cited above, § 68 and *Weber and Saravia*, cited above, § 32).

340. This does not mean that selectors and search criteria need to be made public; nor does it mean that they necessarily need to be listed in the warrant ordering interception. In fact, in the *Liberty* proceedings the IPT found that the inclusion of the selectors in the warrant or accompanying certificate would “unnecessarily undermine and limit the operation of the warrant and be in any event entirely unrealistic” (see paragraph 44 above). The Court has no reason to call this conclusion into question. Nevertheless, the search criteria and selectors used to filter intercepted communications should be subject to independent oversight; a safeguard which appears to be absent in the section 8(4) regime. Indeed, the ISC report criticised the absence of any meaningful oversight of both the selectors and search criteria (see paragraph 157 above).

341. As a result of the application of selectors and automated searches, an index is generated. Material not on the index is discarded. Only material on the index may be examined by an analyst, and only if it satisfies the two criteria in section 16 of RIPA, namely certification by the Secretary of State as to necessity (section 16(1); see paragraphs 78-85 above) and presence for the time being in the British Islands (section 16(2)).

342. As regards the certification by the Secretary of State, the ISC observed that the categories set out in the certificates were set out in very general terms (for example, “material providing intelligence on terrorism (as defined by the Terrorism Act 2000 (as amended)) including, but not limited to, terrorist organisations, terrorists, active sympathisers, attack planning, fund-raising”) (see paragraph 156 above). Similarly, the Independent Reviewer of Terrorism Legislation recommended that the purposes for which material or data was sought should be spelled out by reference to specific operations or mission purposes (for example, “attack planning by ISIL in Iraq/Syria against the UK”) (see paragraph 162 above). In order for this safeguard to be effective, the Court agrees that it would be highly desirable for the certificate to be expressed in more specific terms than it currently appears to be.

343. On the other hand, the exclusion of communications of individuals known currently to be in the British Islands is, in the opinion of the Court, an important safeguard, since persons of interest to the intelligence services who are known to be in the British Islands could be subject to a targeted warrant under section 8(1) of RIPA. The intelligence services should not be permitted to obtain via a bulk warrant what they could obtain via a targeted warrant.

344. According to paragraph 7.18 of the IC Code, periodic audits should be carried out to ensure that the requirements set out in section 16 of RIPA are being met and any breaches of safeguards should be notified to the Interception of Communications Commissioner (see paragraph 90 above). In his 2016 annual report, echoing comments also made in his 2014 and 2015 reports, the Commissioner observed that the process by which analysts selected material for examination, which did not require pre-authorisation by a more senior operational manager, relied mainly on the professional judgment of analysts, their training and subsequent management oversight (see paragraph 179 above).

345. On balance, the Court agrees that it would be preferable for the selection of material by analysts to be subject at the very least to pre-authorisation by a senior operational manager. However, given that analysts are carefully trained and vetted, records are kept and those records are subject to independent oversight and audit (see paragraph 7.15 and 7.18 of the IC Code, at paragraph 90 above), the absence of pre-authorisation would not, in and of itself, amount to a failure to provide adequate safeguards against abuse.

346. Nevertheless, the Court must have regard to the operation of the section 8(4) regime as a whole, and in particular the fact that the list from which analysts are selecting material is itself generated by the application of selectors and selection criteria which were not subject to any independent oversight. In practice, therefore, the only independent oversight of the process of filtering and selecting intercept data for examination is the *post factum* audit by the Interception of Communications Commissioner and, should an application be made to it, the IPT. In *Kennedy* the Court held that the RIPA procedure for examining intercept material was sufficiently clear. That finding, however, was expressly based on the fact that unlike the regime examined in *Liberty and Others*, which concerned the indiscriminate capturing of data, that case was concerned with an interception warrant for one set of premises only; a fact which in and of itself limited the scope of the authorities' discretion to intercept and listen to private communications (see *Kennedy*, cited above, § 162). In a bulk interception regime, where the discretion to intercept is not significantly curtailed by the terms of the warrant, the safeguards applicable at the filtering and selecting for examination stage must necessarily be more robust.

347. Therefore, while there is no evidence to suggest that the intelligence services are abusing their powers – on the contrary, the Interception of Communications Commissioner observed that the selection procedure was carefully and conscientiously undertaken by analysts (see paragraph 179 above) –, the Court is not persuaded that the safeguards governing the selection of bearers for interception and the selection of intercepted material for examination are sufficiently robust to provide adequate guarantees against abuse. Of greatest concern, however, is the absence of robust independent oversight of the selectors and search criteria used to filter intercepted communications.

- The exemption of related communications data from the safeguards applicable to the searching and examining of content

348. The Article 8(4) regime permits the bulk interception of both content and related communications data (the latter being the “who, when and where” of a communication). However, section 16 applies only to “intercepted material” which, according to the interpretation provision in section 20 of RIPA, is defined as the content of intercepted communications (see paragraph 78 above). The related communications data of all intercepted communications – even internal communications incidentally intercepted as a “by-catch” of a section 8(4) warrant – can therefore be searched and selected for examination without restriction.

349. The Government contend that access to communications data is necessary to give effect to one of the section 16 safeguards, namely to determine whether a person is or is not in the British Islands. They further contend that as communications data is less intrusive than data relating to content (at least when compared on a like-for-like basis), its interception, storage and use should not be subject to the same six minimum requirements (see paragraph 307 above). Instead, the Court should simply ask whether the law was sufficiently clear to give the individual adequate protection against arbitrary interference.

350. The Court has distinguished between different methods of investigation which result in different levels of intrusion into an individual’s private life. According to the Court, the interception of communications represents one of the gravest intrusions, as it is capable of disclosing more information on a person’s conduct, opinions or feelings (see *Uzun v. Germany*, no. 35623/05, § 52, ECHR 2010 (extracts)). Consequently, in *Uzun* the Court found that the interception of communications represented a greater intrusion into an individual’s private life than the tracking of his vehicle via GPS (see *Uzun*, cited above, § 52). In *Ben Faiza v. France*, no. 31446/12, 8 February 2018, it further distinguished between the tracking of a vehicle, which nevertheless made it possible to geolocate a person in real time, and the lower level of intrusion occasioned by the transmission to

a judicial authority of existing data held by a public or private body (see *Ben Faiza*, cited above, § 74).

351. However, thus far the Court has only declined to apply the minimum requirements test in secret surveillance cases which did not involve the interception of communications, and in which the degree of intrusion was not considered to be comparable to that caused by interception (see for example, *R.E. v. the United Kingdom*, no. 62498/11, 27 October 2015 and *Uzun*, cited above).

352. In any event, it is not necessary for the Court to decide whether the six minimum requirements apply to the interception of communications data since, save for the section 16 safeguards, the section 8(4) regime treats intercepted content and related communications data in the same way. It will therefore focus its attention on whether the justification provided by the Government for exempting related communications data from this safeguard is proportionate to the legitimate aim pursued; that is, ensuring the effectiveness of that safeguard in respect of content.

353. It is not in doubt that communications data is a valuable resource for the intelligence services. It can be analysed quickly to find patterns that reflect particular online behaviours associated with activities such as a terrorist attack and to illuminate the networks and associations of persons involved in such attacks, making it invaluable in fast-moving operations; and, unlike much data relating to content, it is not generally encrypted (see paragraphs 158, 163, 169, 176 and 301 above).

354. Furthermore, the Court accepts that the effectiveness of the section 16(2) safeguard depends on the intelligence services having a means of determining whether a person is in the British Islands, and access to related communications data would provide them with that means.

355. Nevertheless, it is a matter of some concern that the intelligence services can search and examine “related communications data” apparently without restriction. While such data is not to be confused with the much broader category of “communications data”, it still represents a significant quantity of data. The Government confirmed at the hearing that “related communications data” obtained under the section 8(4) regime will only ever be traffic data. However, according to paragraphs 2.24-2.27 of the ACD Code (see paragraph 117 above), traffic data includes information identifying the location of equipment when a communication is, has been or may be made or received (such as the location of a mobile phone); information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or attached to the communication; routing information identifying equipment through which a communication is or has been transmitted (for example, dynamic IP address allocation, file transfer logs and e-mail headers (other than the subject line of an e-mail, which is classified as content)); web browsing information to the extent that only a host machine, server, domain name or IP address is disclosed (in

other words, website addresses and Uniform Resource Locators (“URLs”) up to the first slash are communications data, but after the first slash content); records of correspondence checks comprising details of traffic data from postal items in transmission to a specific address, and online tracking of communications (including postal items and parcels) (see paragraph 117 above).

356. In addition, the Court is not persuaded that the acquisition of related communications data is necessarily less intrusive than the acquisition of content. For example, the content of an electronic communication might be encrypted and, even if it were decrypted, might not reveal anything of note about the sender or recipient. The related communications data, on the other hand, could reveal the identities and geographic location of the sender and recipient and the equipment through which the communication was transmitted. In bulk, the degree of intrusion is magnified, since the patterns that will emerge could be capable of painting an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with (see paragraph 301 above).

357. Consequently, while the Court does not doubt that related communications data is an essential tool for the intelligence services in the fight against terrorism and serious crime, it does not consider that the authorities have struck a fair balance between the competing public and private interests by exempting it in its entirety from the safeguards applicable to the searching and examining of content. While the Court does not suggest that related communications data should only be accessible for the purposes of determining whether or not an individual is in the British Islands, since to do so would be to require the application of stricter standards to related communications data than apply to content, there should nevertheless be sufficient safeguards in place to ensure that the exemption of related communications data from the requirements of section 16 of RIPA is limited to the extent necessary to determine whether an individual is, for the time being, in the British Islands.

- *Duration of the secret surveillance measure*

358. Pursuant to section 9 of RIPA (see paragraph 62 above), a section 8(4) warrant ceases to have effect at the end of the “relevant period” unless it is renewed. For warrants issued by the Secretary of State for reasons of national or economic security, the “relevant period” is six months, and for warrants issued by the Secretary of State for the purposes of preventing serious crime, the “relevant period” is three months. These warrants are renewable for periods of six and three months respectively. Warrants may be renewed at any point before their expiry date by application to the Secretary of State. The application must contain the same

information as the original application; it must also contain an assessment of the value of the interception to date and explain why the continuation of interception is necessary, within the meaning of section 5(3), and proportionate (see paragraph 6.22-6.24 of the IC Code at paragraph 90 above). Paragraph 6.7 of the IC Code requires regular surveys of relevant communications links (see paragraph 90 above). Consequently, any application for renewal of a warrant would have to show that interception of those links continued to be of value, and continued to be necessary and proportionate (in the Convention sense).

359. Furthermore, the Secretary of State must cancel a warrant if satisfied that it is no longer necessary on section 5(3) grounds (see section 9 of RIPA at paragraph 62 above).

360. In *Kennedy* (cited above, § 161) the Court considered the same provisions on the duration and renewal of interception warrants (in that case, in the context of the section 8(1) regime) and found that the rules were sufficiently clear as to provide adequate safeguards against abuse. In particular, it noted that the duty on the Secretary of State to cancel warrants which were no longer necessary meant, in practice, that the intelligence services had to keep their warrants under continuous review. In light of the foregoing considerations, the Court sees no grounds upon which to reach a different conclusion in the present case. In particular, it sees no evidence to substantiate the applicants' claim that once issued, section 8(4) warrants could continue indefinitely regardless of whether they continued to be necessary and proportionate.

- Procedure to be followed for storing, accessing, examining and using the intercepted data

361. As already noted, analysts may only examine material which appears on the automatically generated index. Prior to analysts being able to read, look at or listen to material on the index, they must make a record of why access to the material is necessary for one of the statutory purposes set out in section 5(3) of RIPA, and proportionate, having regard to whether the information could reasonably be obtained by less intrusive means (see section 16 of RIPA, at paragraph 79 above, and paragraph 7.15 of the IC Code, at paragraph 90 above). Pursuant to section 16(2), they cannot select material for examination using criteria that refer to the communications of individuals known currently to be in the British Islands (see paragraph 79 above). Paragraph 7.16 of the IC Code also requires the analyst to indicate any circumstances likely to give rise to a degree of collateral infringement of privacy, together with the measures taken to reduce the extent of that intrusion (see paragraph 90 above). Subsequent access by the analyst is limited to a defined period of time; although that period of time may be renewed, the record must be updated giving reasons for renewal (see paragraph 7.17 of the IC Code, at paragraph 90 above).

362. Paragraph 7.15 of the IC Code further requires that analysts examining intercepted material must be specially authorised to do so; must receive regular mandatory training regarding on the provisions of RIPA and specifically the operation of section 16 and the requirements of necessity and proportionality; and must be vetted (see paragraph 90 above). Furthermore, regular audits are carried out which must include checks to ensure that the records requesting access to material have been compiled correctly, and that the material requested falls within the matters certified by the Secretary of State (see paragraph 7.18 of RIPA, at paragraph 90 above).

363. With regard to the storage of intercepted material, paragraph 7.7 of the IC Code requires that prior to its destruction, it must be stored securely and must not be accessible to persons without the required level of security clearance (see paragraph 90 above).

364. In light of the foregoing, and subject to its conclusions at paragraph 347 and 357 above, the Court would accept that the provisions relating to the storing, accessing, examining and using intercepted data are sufficiently clear.

- Procedure to be followed for communicating the intercepted data to other parties

365. While material is being stored, section 15(2) of RIPA and paragraphs 7.2 of the IC Code require that the following are limited to the minimum necessary for the “authorised purposes”: the number of persons to whom the material or data is disclosed or made available; the extent to which the material or data is disclosed or made available; the extent to which the material or data is copied; and the number of copies that are made (see paragraphs 72-77 and 90 above). Pursuant to section 15(4) and paragraph 7.2 of the IC Code, something is necessary for the authorised purposes if, and only if, it continues to be, or is likely to become, necessary for the purposes mentioned in section 5(3) of RIPA; for facilitating the carrying out of any of the interception functions of the Secretary of State; for facilitating the carrying out of any functions of the Interception of Communications Commissioner or of the IPT; to ensure 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; or for the performance of any duty imposed on any person under public records legislation (see paragraphs 72-77 and 90 above).

366. Paragraph 7.3 of the IC Code prohibits disclosure to persons who have not been appropriately vetted 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 or she needs to know about the intercepted material to carry out those duties (see paragraph 90 above). In the same way, only so much of the intercepted material may be disclosed as the recipient needs. Paragraph 7.3 applies

equally to disclosure to additional persons within an agency, and to disclosure outside the agency. Pursuant to paragraph 7.4, it also applies not just to the original interceptor, but also to anyone to whom the intercepted material is subsequently disclosed (see paragraph 90 above).

367. According to paragraph 7.5 of the IC Code, where intercepted material is disclosed to the authorities of a country or territory outside the United Kingdom, 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. 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 (see paragraph 90 above).

368. The Court considered very similar provisions in *Kennedy*; although paragraph 7.5 is new, paragraphs 7.3, 7.4 and 7.6 in the 2016 IC Code are identical to paragraphs 6.4, 6.5 and 6.6 of the previous version. It was satisfied that the provisions on processing and communication of intercept material provided adequate safeguards for the protection of data obtained (see *Kennedy*, cited above, § 163). In the present case, however, the applicants have expressed concern about an aspect of the procedure which was not addressed in *Kennedy*; namely, the requirement that disclosure and copying be “limited to the minimum necessary for the ‘authorised purposes’”, when something might be considered “necessary” for an “authorised purpose” if it was “likely to become necessary”. As “likely to become necessary” is not further defined in RIPA or the IC Code, or indeed anywhere else, it could in practice give the authorities a broad power to disclose and copy intercept material. Nevertheless, it is clear that even if disclosure or copying is “likely to become necessary” for an “authorised purpose”, the material can still only be disclosed to a person with the appropriate level of security clearance, who has a “need to know”. Furthermore, only so much of the intercept material as the individual needs to know is to be disclosed; where a summary of the material would suffice, then only a summary should be disclosed.

369. Therefore, while it would be desirable for the term “likely to become necessary” to be more clearly defined in either RIPA or the IC Code, the Court considers that, taken as a whole, section 15 of RIPA and Chapter 7 of the IC Code provide adequate safeguards for the protection of data obtained.

- The circumstances in which intercept material must be erased or destroyed

370. Section 15(3) of RIPA and paragraph 7.8 of the IC Code require that every copy of intercepted material or data (together with any extracts

and summaries) be destroyed securely as soon as retention is no longer necessary for any of the section 5(3) purposes (see paragraphs 74 and 90 above). In practice, this means that intercepted material which is filtered out in near real-time is destroyed. Similarly, following the application of selectors and search criteria, material which is not added to the analyst's index is also destroyed (see paragraphs 72-77 and 90 above).

371. Paragraph 7.9 provides that where an intelligence service receives unanalysed intercepted material and related communications data from interception under a section 8(4) warrant, it must specify maximum retention periods for different categories of the data which reflect its nature and intrusiveness. These specified periods should normally be no longer than two years, and should be agreed with the Interception of Communications Commissioner. 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 (see paragraphs 72-77 above). Pursuant to paragraph 7.8, if intercepted 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 (see paragraph 90 above).

372. According to the 2016 annual report of the Interception of Communications Commissioner, every interception agency had a different view on what constituted an appropriate retention period for intercepted material and related communications data. The retention periods for content ranged between thirty days and one year and the retention periods for related communications data ranged between six months and one year (see paragraph 186 above). Therefore, while the specific retention periods are not in the public domain, it is clear that they cannot exceed two years and, in practice, they do not exceed one year (with much content and related communications data being retained for significantly shorter periods).

373. Furthermore, where an application is lodged with the IPT, it can examine whether the time-limits for retention have been complied with and, if they have not, it may find that there has been a breach of Article 8 of the Convention and order the destruction of the relevant material. Where the retention has resulted in damage, detriment or prejudice, compensation may also be awarded. In the *Liberty* proceedings, brought by the applicants in the third of the joined cases, the IPT found that there had been a breach of Article 8 of the Convention by virtue of the fact that email communications of Amnesty International, which had been intercepted and accessed "lawfully and proportionately", had nevertheless been retained for longer than was permitted under GCHQ's internal policies. GCHQ was ordered to destroy the communications within seven days, and to provide a closed report within fourteen days confirming their destruction. A hard copy of the communications was to be delivered to the Commissioner (see paragraph 54 above).

374. Therefore, in the Court's view the provisions on the erasure and destruction of intercept material are also sufficiently clear.

- *Supervision, notification and remedies*

375. Supervision of the regime is carried out at a number of levels. First of all, according to the Interception of Communications Commissioner, a "critical quality assurance function [is] initially carried out by the staff and lawyers within the intercepting agency or the warrant-granting department" (see paragraph 180 above). The warrant-granting departments provide independent advice to the Secretary of State and perform important pre-authorisation scrutiny of warrant applications and renewals to ensure that they were (and remained) necessary and proportionate (see paragraph 180 above).

376. Secondly, section 8(4) warrants must be authorised by the Secretary of State. As already noted, while the Court has recognised judicial authorisation to be an "important safeguard against arbitrariness" (see *Roman Zakharov*, cited above, § 249), to date it has not considered it to be a "necessary requirement" (see, for example, *Roman Zakharov*, cited above, § 258; see also *Klass and Others*, cited above, § 51; *Weber and Saravia*, cited above, § 115; *Kennedy*, cited above, § 31; and *Szabó and Vissy*, cited above, § 77). Although desirable in principle, by itself it is neither necessary nor sufficient to ensure compliance with Article 8 of the Convention (see paragraphs 318-320 above).

377. It is true that the Court has generally required a non-judicial authority to be sufficiently independent of the executive (see *Roman Zakharov*, cited above, § 258). However, it must principally have regard to the actual operation of a system of interception as a whole, including the checks and balances on the exercise of power, and the existence (or absence) of any evidence of actual abuse (see paragraph 320 above), such as the authorising of secret surveillance measures haphazardly, irregularly or without due and proper consideration (see *Roman Zakharov*, cited above, § 267).

378. In the present case there is no evidence to suggest that the Secretary of State was authorising warrants without due and proper consideration. The authorisation procedure was subject to independent oversight by the Interception of Communications Commissioner (recently replaced by the Investigatory Powers Commissioner following the coming into force of the Investigatory Powers Act 2016 – see paragraph 147 above), who was independent of the executive and the legislature, held or had held high judicial office, and was tasked with overseeing the general functioning of the surveillance regime and the authorisation of interception warrants in specific cases. The Commissioner reported annually to the Prime Minister and his report was a public document (subject to the non-disclosure of confidential annexes) which was laid before Parliament. In undertaking his

review of surveillance practices, he was granted access to all relevant documents, including closed materials, and all those involved in interception activities had a duty to disclose to him any material he required. The obligation on the intelligence services to keep records ensured that he had effective access to details of surveillance activities undertaken (see paragraph 145 above). In 2016, 970 warrants were examined during twenty-two interception inspections, representing 61% of the number of warrants in force at the end of the year and 32% of the total of new warrants issued in 2016 (see paragraph 185 above). As a consequence, in *Kennedy* the Court accepted that despite the fact that the section 8(1) warrant was authorised by the Secretary of State, sufficient independence was provided by the Interception of Communications Commissioner (see *Kennedy*, cited above, § 166).

379. Furthermore, the IPT has extensive jurisdiction to examine any complaint of unlawful interception: unlike in many other countries, its jurisdiction does not depend on notification of the interception to its subject (see paragraph 124 above), which means that any person who believes that he or she has been subject to secret surveillance may make an application to it (see paragraph 318 above). Its members must hold or have held high judicial office or be a qualified lawyer of at least ten years' standing (see paragraph 123 above). Those involved in the authorisation and execution of an intercept warrant are required to disclose to it all the documents it may require, including "below the waterline" documents which could not be made public for reasons of national security (see paragraph 127 above); it has discretion to hold oral hearings, in public, where possible (see paragraphs 131, 138 and 139 above); in closed proceedings it may appoint Counsel to the Tribunal also to make submissions on behalf of claimants who cannot be represented (see paragraph 142 above); and when it determines a complaint it has the power to award compensation and make any other order it sees fit, including quashing or cancelling any warrant and requiring the destruction of any records (see paragraph 128 above). The publication of the IPT's legal rulings further enhances the level of scrutiny afforded to secret surveillance activities in the United Kingdom (see *Kennedy*, cited above, § 167).

380. In any case, the Court notes that under the new Investigatory Powers Act 2016 warrants will have to be approved by judicial commissioners following their authorisation by the Secretary of State. Although this new procedure has not yet been implemented, the Investigatory Powers Commissioner and the deputy Investigatory Powers Commissioner have been appointed (see paragraph 197 above).

381. Therefore, while the Court considers judicial authorisation to be highly desirable and, in its absence, will generally require a non-judicial authority to be independent of the executive, in the present case, in view of the pre-authorisation scrutiny of warrant applications, the extensive post-

authorisation scrutiny provided by the (independent) Commissioner's office and the IPT, and the imminent changes to the impugned regime, it would accept that the authorisation of section 8(4) warrants by the Secretary of State does not, in and of itself, give rise to a breach of Article 8 of the Convention.

382. Finally, the Court recalls that in light of the Edward Snowden revelations, there were three thorough independent reviews of the existing interception regimes, and none of the reviewing bodies found any evidence that deliberate abuse of interception powers was taking place (see paragraphs 148-172 above).

383. In light of the above considerations, the Court is of the opinion that the supervision and oversight of the bulk interceptions capable of providing adequate and effective guarantees against abuse.

- *Proportionality*

384. With regard to the proportionality of the bulk interception regime, the Court notes that the Independent Reviewer of Terrorism Legislation, examined a great deal of closed material and concluded that bulk interception was an essential capability: first, because terrorists, criminals and hostile foreign intelligence services had become increasingly sophisticated at evading detection by traditional means; and secondly, because the nature of the global Internet meant that the route a particular communication would travel had become hugely unpredictable. Although he and his team (including a person with the necessary technical background to understand the systems and techniques used by GCHQ, and the uses to which they could be put, an investigator with experience as a user of secret intelligence, including intelligence generated by GCHQ, and senior independent counsel with the skills and experience to challenge forensically the evidence and the case studies presented by the security and intelligence services) looked at alternatives to bulk interception (including targeted interception, the use of human sources and commercial cyber-defence products), they concluded that no alternative or combination of alternatives would be sufficient to substitute for the bulk interception power (see paragraph 176 above).

385. Similarly, while acknowledging the risks that bulk interception can pose for individual rights, the Venice Commission nevertheless recognised its intrinsic value for security operations, since it enabled the security services to adopt a proactive approach, looking for hitherto unknown dangers rather than investigating known ones (see paragraph 211 above).

386. The Court sees no reason to disagree with the thorough examinations carried out by these bodies and the conclusions subsequently reached. It is clear that bulk interception is a valuable means to achieve the legitimate aims pursued, particularly given the current threat level from both global terrorism and serious crime.

150 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

(γ) Conclusions

387. In light of the foregoing considerations, the Court considers that the decision to operate a bulk interception regime was one which fell within the wide margin of appreciation afforded to the Contracting State. Furthermore, in view of the independent oversight provided by the Interception of Communications Commissioner and the IPT, and the extensive independent investigations which followed the Edward Snowden revelations, it is satisfied that the intelligence services of the United Kingdom take their Convention obligations seriously and are not abusing their powers under section 8(4) of RIPA. Nevertheless, an examination of those powers has identified two principal areas of concern; first, the lack of oversight of the entire selection process, including the selection of bearers for interception, the selectors and search criteria for filtering intercepted communications, and the selection of material for examination by an analyst; and secondly, the absence of any real safeguards applicable to the selection of related communications data for examination.

388. In view of these shortcomings and to the extent just outlined, the Court finds that the section 8(4) regime does not meet the “quality of law” requirement and is incapable of keeping the “interference” to what is “necessary in a democratic society”. There has accordingly been a violation of Article 8 of the Convention.

B. The intelligence sharing regime

389. The applicants in the third of the joined cases complain that the respondent State’s receipt of material intercepted by the NSA under PRISM and Upstream was in breach of their rights under Article 8 of the Convention. The applicants in the first of the joined cases complain more generally about the receipt of information from foreign intelligence services.

1. Admissibility

(a) The parties’ submissions

390. The Government argued that the applicants could not claim to be victims of the alleged violation within the meaning of Article 34 of the Convention since they could not possibly have been affected by the intelligence sharing regime. They did not contend, and had put forward no evidential basis for contending, that their communications had in fact been intercepted under PRISM/Upstream and subsequently shared with the United Kingdom intelligence services. Rather, they asserted only that their communications “might have been” subject to foreign interception conveyed to United Kingdom authorities, or that they “believed” that to be the case. As such, their complaint was an abstract one about the regime

itself, and the Court should not entertain an abstract challenge when the applicants had available to them an effective remedy in the form of the IPT.

391. The applicants, on the other hand, submitted that on account of their global public interest activities and the very broad range of persons and organisations with which they were in contact, they were at genuine risk of having their communications obtained by a foreign intelligence service and requested by the United Kingdom authorities. They further submitted that there was no adequate remedy available under domestic law for the alleged breach of their Convention rights.

(b) The Court's assessment

392. The Court has accepted that an applicant could 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 were satisfied: first, the Court would examine whether the applicant could possibly be affected by the legislation permitting secret surveillance measures; and secondly, it would take into account the availability of remedies at the national level and adjust the degree of scrutiny depending on the effectiveness of such remedies. Where the domestic system did not afford an effective remedy, there would be a greater need for scrutiny by the Court and the individual would not need to demonstrate the existence of any risk that secret surveillance measures were applied to him. By contrast, if the national system provides for effective remedies, the individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or of 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 (*Roman Zakharov*, cited above, § 171).

393. In the present case the Court has accepted that the IPT offers an effective remedy to anyone who wishes to complain about an interference with his or her communications by the United Kingdom authorities (see paragraphs 250-266 above). It has jurisdiction to investigate any complaint that a person's communications have been intercepted and, where interception has occurred, to examine the authority for such interception (see paragraph 124 above). This jurisdiction clearly extends to complaints about the receipt of intelligence from foreign intelligence services. Indeed, in the *Liberty* proceedings the IPT considered the applicants' complaints about both the section 8(4) regime and the intelligence sharing regime with equal diligence (see paragraphs 32-40 above). Consequently, the applicants can only claim to be "victims" on account of the mere existence of the intelligence sharing regime if they are able to show that, due to their personal situation, they were potentially at risk of having their communications obtained by the United Kingdom authorities through a

request to a foreign intelligence service (see *Roman Zakharov*, cited above, § 171).

394. According to Chapter 12 of the IC Code, absent exceptional circumstances intelligence can only be requested from third countries where there is already a section 8(1) or section 8(4) warrant in place. This means that there must either be an Article 8(1) warrant in relation to the subject at issue, or a section 8(4) warrant and accompanying certificate which covers the subject's communications (see paragraph 90 above). However, section 8(4) warrants are relatively broad in scope, and the Court has already considered the general terms in which both warrants and accompanying certificates are drafted (see paragraphs 156 and 341 above). Moreover, it is clear from the *Liberty* proceedings that at least two of the applicants in the third of the joined cases had their communications lawfully intercepted and selected for examination by the United Kingdom intelligence services under the section 8(4) regime (see paragraphs 54 and 55 above). While there is no reason to believe that these applicants were themselves of interest to the intelligence services, their communications could have been obtained lawfully under the section 8(4) regime if, as they claim, they were in contact with persons who were. Similarly, their communications could lawfully be requested from a third country under the intelligence sharing regime if they were in contact with an individual who was the subject of a request.

395. The Court would therefore accept, on the basis of the information submitted to it, that the applicants were potentially at risk of having their communications requested from a foreign intelligence service. In addition, it would accept that they were also potentially at risk of having their communications obtained by a foreign intelligence service. Although the United States of America is not the only country from which the authorities of the respondent State might request intelligence, the submissions before this Court – and before the IPT – focused on the receipt of information from the NSA. While PRISM is a targeted scheme which allows intelligence material to be obtained from Internet Service Providers (“ISPs”), Upstream appears to be a bulk interception scheme similar to the section 8(4) regime. In other words, it permits broad access to global data, in particular that of non-US citizens, which can then be collected, stored and searched using keywords.

396. In light of the foregoing considerations, the Court would accept that the applicants were potentially at risk of having their communications obtained by the intelligence services of the respondent State under the intelligence sharing regime. As such, it finds that they can claim to be victims, within the meaning of Article 34 of the Convention, of the violation alleged to flow from the intelligence sharing regime.

397. The Court notes that this complaint is not manifestly ill-founded within the meaning of Article 35 § 3 (a) of the Convention. It further notes

that it is not inadmissible on any other grounds. It must therefore be declared admissible.

2. *Merits*

(a) **The parties' submissions**

(i) *The applicants*

398. The applicants submitted that even following the 9 October disclosure, there remained no basis in law for the intelligence sharing carried out by the intelligence services, and there was certainly no regime which satisfied the Court's "quality of law" requirements.

399. With regard to the test to be applied, the applicants contended that an interference with the rights protected by Article 8 of the Convention was no less serious when a third State shared the intelligence with the respondent State than when the respondent State conducted the surveillance itself. In *R.E.* the Court held that in determining whether the six minimum requirements applied the decisive factor would be the level of interference with an individual's right to respect for his or private life, and not the technical definition of that interference (*R.E.*, cited above, § 130). Since the degree of interference caused by the receipt of intelligence from third countries was similar to that caused by direct interception on the part of the respondent State, how that interference was technologically achieved should be irrelevant.

400. In the opinion of the applicants, the publication of the revised IC Code in 2016 was insufficient the remedy the flaws in the regime identified by the IPT as it simply applied the inadequate RIPA regime to the obtaining of data intercepted by a foreign Government.

(ii) *The Government*

401. The Government submitted that the intelligence sharing regime now had a basis in domestic law (namely, the Security Services Act 1989 ("the SSA") and the Intelligence Services Act 1994 ("the ISA"), as read with the Counter Terrorism Act 2008 ("the CTA"); the Human Rights Act 1998 ("the HRA"); the Data Protection Act 1998 ("the DPA"); the Official Secrets Act 1989 ("the OSA"); and Chapter 12 of the IC Code) and that law was clearly accessible.

402. They further argued that it was foreseeable as the law indicated the scope of any discretion and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference. They did not accept that the six criteria set down in *Weber and Saravia* (see paragraph 307 above) applied to an intelligence sharing regime in the same way as they applied to an interception regime. In this regard, the Court had expressly recognised that the strict standards developed in intercept cases

did not necessarily apply in other surveillance cases (for example, *Uzun*, cited above). While some of the material obtained from foreign governments might be the product of intercept, that would not necessarily be the case and the intelligence services might not even know whether communications provided to them by a foreign Government were the product of intercept.

403. Even if the six minimum requirements did apply, the Government argued that they were satisfied. First, the regime was sufficiently clear as regards the circumstances in which the intelligence services could in principle obtain information from other States; they could only obtain information so far as it was necessary for the proper discharge of their functions, being the interests of national security, the economic well-being of the United Kingdom, and the prevention and detection of serious crime.

404. Moreover, the circumstances in which the intelligence agencies could obtain information under the intelligence sharing regime were defined and circumscribed by the IC Code. In this regard, the effect of Chapter 12 of the Code was to confirm that, other than in exceptional circumstances, the intelligence services could only request “raw intercept” from a foreign government if it concerned targets who were already the subject of an interception warrant under Part I of RIPA, that material could not be obtained by the intelligence services themselves, and it was necessary and proportionate to obtain it. In the absence of a warrant, a request could only be made if it did not amount to a deliberate circumvention, or otherwise frustrate the objectives, of RIPA. Furthermore, any request made in the absence of a warrant would be decided on by the Secretary of State personally, and if the request was for “untargeted” material, communications obtained could not be examined according to any of the factors mentioned in section 16(2) of RIPA.

405. The Government further contended that the intelligence sharing regime was sufficiently clear as regards the subsequent handling, use and possible onward disclosure of material. Not only were the intelligence services bound by the general constraints of proportionality in the HRA and the fifth and seventh data protection principles, but Chapter 12 of the IC Code also provided that intercepted communications data or content received from another State, regardless of whether it was solicited or unsolicited, analysed or unanalysed, was subject to exactly the same rules and safeguards as material obtained directly by the intelligence services by interception under RIPA. In other words, the safeguards set out in section 15 of RIPA also applied to intercept material obtained under the intelligence sharing regime.

406. Finally, the Government pointed out that the intelligence sharing regime was subject to the same oversight mechanisms as the section 8(4) regime, and none of these oversight bodies had revealed any deliberate abuse by the intelligence services of their powers. Furthermore, no evidence

was found to suggest that the intelligence services had – or had attempted – to use the intelligence sharing regime to circumvent RIPA.

(b) The submissions of the third parties

(i) The Electronic Privacy Information Center (“EPIC”)

407. EPIC submitted that the evolving technologies of the NSA and other intelligence agencies had created an almost unlimited ability to access, store and use personal information and private communications globally. However, no US law or regulation prohibited the NSA from conducting warrantless surveillance on foreign citizens abroad. Furthermore, in recent years the US had failed to adopt any meaningful reforms which would have provided adequate privacy and data protection safeguards for non-US persons.

(ii) Access Now

408. Access Now contended that while Mutual Legal Assistance Treaties (“MLATs”) offered a transparent and formal process for one State party to request intelligence for another, the operation of secret signals intelligence programmes (for example, the Five Eyes intelligence sharing network of which the United Kingdom, the US, Australia, Canada and New Zealand were members) were not transparent and were prohibited by international human rights standards. Such secret programmes were not necessary, since the relevant intelligence could be obtained under MLATs.

(iii) Bureau Brandeis

409. The members of the Bureau Brandeis coalition were plaintiffs in a case against the Netherlands. The Dutch authorities had accepted that data was exchanged with foreign intelligence partners (including the US) and that it could not be excluded that they had received information acquired by foreign services using methods that might infringe human rights. The coalition brought proceedings in which they argued that the NSA’s mass data collection programs violated human rights guaranteed by the Convention. However, the Hague District Court said that under Dutch law, Dutch intelligence services were allowed to collaborate with the NSA, and the NSA was in turn bound by US law which, in general, did not conflict with the Convention’s privacy requirements. The court further held that because the raw data was shared in bulk, less stringent safeguards were necessary than would apply when the data was examined and used, as there was a difference between receiving data and using it for individual cases. An appeal against this decision was dismissed in March 2017.

410. In their third party intervention before this Court, the coalition argued that the sharing of intelligence should only be permitted if it was accompanied by sufficient safeguards and the foreign authority had a sound

156 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

legal basis for capturing the material. Otherwise, there could be a circumvention of the protection provided by Article 8 of the Convention. In other words, States should not be allowed to obtain material from foreign authorities that they could not lawfully capture themselves.

(iv) *Center for Democracy and Technology (“CDT”) and Pen American Center (“PEN America”)*

411. CDT and PEN America submitted that the interception regimes operated by the NSA would satisfy neither the “in accordance with the law” nor the “proportionality” requirements of Article 8 of the Convention, and these deficiencies tainted the lawfulness of the United Kingdom’s intelligence sharing regime.

(v) *The International Commission of Jurists (“ICJ”)*

412. The ICJ referred the Court to Articles 15 and 16 of the Articles of State Responsibility of the International Law Commission (“the ILC Articles”). They contended that, pursuant to Article 15, a Contracting State could be responsible for mass surveillance conducted by a non-Contracting State if they were acting in organised and structured forms of co-operation; and that, pursuant to Article 16, a Contracting State could be responsible for mass surveillance conducted by a non-Contracting State if it contributed to the surveillance programme and had actual or constructive knowledge of the breaches of international human rights obligations inherent in the system. The ICJ further submitted that Contracting States participating in or contributing to a mass surveillance programme were obliged to establish a system of safeguards for the protection of Article 8 rights, and were also under a duty to protect persons within their jurisdiction from violations of Article 8 rights caused by mass surveillance programmes.

(vi) *Open Society Justice Initiative (“OSJI”)*

413. OSJI argued that States should not receive or request data from a third party in a manner that circumvents individuals’ Article 8 rights. To ensure that this does not happen, they must put in place safeguards at the point when the material is first gathered, including prior scrutiny of the human rights record and interception laws and practices in the foreign State, and independent, preferably judicial, *a posteriori* oversight of any sharing arrangements to ensure that the safeguards are in place and enforced.

(vii) *The Law Society of England and Wales*

414. The Law Society previously submitted that the RIPA regime and associated Codes provided no robust or transparent safeguards for legally privileged material. Since the same safeguards applied to privileged material obtained by foreign States and disclosed to the intelligence services of the United Kingdom, the same deficiencies also tainted that regime.

(viii) *Human Rights Watch (“HRW”)*

415. Although the present applications focused on the receipt of foreign intelligence from the United States, HRW believed that the network of States with which communications intelligence was shared was vastly larger. For example the “Five Eyes Alliance” comprised the United Kingdom, the United States, Australia, Canada and New Zealand, and there were also thought to be other, more restricted intelligence sharing coalitions (for example, the “Nine Eyes”, adding Denmark, France, the Netherlands and Norway; the “Fourteen Eyes”, adding Germany, Belgium, Italy, Spain and Sweden; and the “Forty-One Eyes”, adding in others in the allied coalition in Afghanistan).

(c) **The Court’s assessment**

(i) *The scope of the applicants’ complaints*

416. This is the first time that the Court has been asked to consider the Convention compliance of an intelligence sharing regime. While the operation of such a scheme might raise a number of different issues under the Convention, in the present case the applicants’ complaints focus on the Article 8 compliance of the regime by which the United Kingdom authorities request and receive intelligence from foreign Governments. The applicants do not complain about the transfer of intelligence from the United Kingdom intelligence services to foreign counterparts; nor do they invoke any other Convention Articles.

417. In the *Liberty* proceedings (in which the IPT was only concerned with the receipt of information from the United States) the applicants submitted that information acquired from the NSA fell into three categories: material which the NSA had provided to the United Kingdom intelligence services unsolicited, and which on its face derived from intercept; communications which the United Kingdom intelligence services had either asked the NSA to intercept, or to make available to them as intercept; and material obtained by the NSA other than by the interception of communications. Although the complaint before the Court is somewhat wider than the one which was before the IPT, the applicants in the first of the joined cases having complained about the receipt of information from any foreign Government, the categories identified by the IPT are nevertheless apposite. As the Government, at the hearing, informed the Court that it was “implausible and rare” for intercept material to be obtained “unsolicited”, the Court will restrict its examination to material falling into the second and third categories.

418. Material falling within the second category can be divided into two sub-categories: communications which the respondent State has asked a foreign intelligence service to intercept; and communications already intercepted by a foreign intelligence service, which are conveyed to the

authorities of the respondent State upon their request. The Court will first deal with these two sub-categories together, before proceeding to consider the third category separately.

(ii) The nature of the interference

419. The Court has already found that the applicants can claim to be victims of the alleged violation of Article 8 of the Convention occasioned by the existence of an intelligence sharing regime. However, it is important to clarify at the outset the nature of the interference under consideration.

420. Although the impugned regime concerns intercepted communications, the interference under consideration in this case does not lie in the interception itself, which did not, in any event, occur within the United Kingdom's jurisdiction, and was not attributable to that State under international law. As the communications are being intercepted by foreign intelligence agencies, their interception could only engage the responsibility of the respondent State if it was exercising authority or control over those agencies (see, for example, *Jaloud v. the Netherlands* [GC], no. 47708/08, §§ 139 and 151 ECHR 2014 and *Al-Skeini and Others v. the United Kingdom* [GC], no. 55721/07, §§ 130-139, ECHR 2011). Even when the United Kingdom authorities request the interception of communications (rather than simply the conveyance of the product of intercept), the interception would appear to take place under the full control of the foreign intelligence agencies. Some of the third parties have invoked the ILC Articles, but these would only be relevant if the foreign intelligence agencies were placed at the disposal of the respondent State and were acting in exercise of elements of the governmental authority of the respondent State (Article 6); if the respondent State aided or assisted the foreign intelligence agencies in intercepting the communications where that amounted to an internationally wrongful act for the State responsible for the agencies, the United Kingdom was aware of the circumstances of the internationally wrongful act, and the act would have been internationally wrongful if committed by the United Kingdom (Article 16); or if the respondent State exercised direction or control over the foreign Government (Article 17). There is no suggestion that this is the case.

421. Consequently, the interference lies in the receipt of the intercepted material and its subsequent storage, examination and use by the intelligence services of the respondent State.

(iii) The applicable test

422. As with any regime which provides for the acquisition of surveillance material, the regime for the obtaining of such material from foreign Governments must be "in accordance with the law"; in other words, it must have some basis in domestic law, it must be accessible to the person concerned and it must be foreseeable as to its effects (see *Roman Zakharov*,

cited above, § 228). Furthermore, it must be proportionate to the legitimate aim pursued, and there must exist adequate and effective safeguards against abuse. In particular, the procedures for supervising the ordering and implementation of the measures in question must be such as to keep the “interference” to what is “necessary in a democratic society” (see *Roman Zakharov*, cited above, § 232).

423. The parties dispute whether the six minimum requirements commonly applied in cases concerning the interception of communications (namely, the nature of offences which may give rise to an interception order; a definition of the categories of people liable to have their communications intercepted; a limit on the duration of interception; 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 intercepted data may or must be erased or destroyed – see paragraph 307 above) should apply in the present case. It is true that the interference in this case is not occasioned by the interception of communications by the respondent State. However, as the material obtained is nevertheless the product of intercept, those requirements which relate to its storage, examination, use, onward dissemination, erasure and destruction must be present. Indeed, as the Venice Commission noted, as States could use intelligence sharing to circumvent stronger domestic surveillance procedures and/or any legal limits which their agencies might be subject to as regards domestic intelligence operations, a suitable safeguard would be to provide that the bulk material transferred could only be searched if all the material requirements of a national search were fulfilled and this was duly authorised in the same way as a search of bulk material obtained by the signals intelligence agency using its own techniques (see paragraph 216 above).

424. Furthermore, while the first and second of the six requirements may not be of direct relevance where the respondent State is not carrying out the interception itself, the Court is nevertheless mindful of the fact that if Contracting States were to enjoy an unfettered discretion to request either the interception of communications or the conveyance of intercepted communications from non-Contracting States, they could easily circumvent their obligations under the Convention. Consequently, the circumstances in which intercept material can be requested from foreign intelligence services must also be set out in domestic law in order to avoid abuses of power. While the circumstances in which such a request can be made may not be identical to the circumstances in which the State may carry out interception itself (since, if a State’s own intelligence services could lawfully intercept communications themselves, they would only request this material from foreign intelligence services if it is not technically feasible for them to do so), they must nevertheless be circumscribed sufficiently to prevent –

160 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

insofar as possible – States from using this power to circumvent either domestic law or their Convention obligations.

(iv) *Application of the test to material falling into the second category*

(α) Accessibility

425. The statutory framework which permits the United Kingdom intelligence services to request intercepted material from foreign intelligence agencies is not contained in RIPA. The British-US Communication Intelligence Agreement of 5 March 1946 specifically permits the exchange of material between the United States and the United Kingdom. More generally, the SSA (see paragraphs 98-99 above) and the ISA (see paragraphs 100-103 above) set out the function of the intelligence services and require that there be arrangements for ensuring that no information is obtained by them except so far as necessary for the proper discharge of their functions; and that no information is disclosed by them except so far as necessary for that purpose or for the purpose of any criminal proceedings.

426. Details of the internal arrangements referred to in the SSA and ISA were disclosed during the *Liberty* proceedings (the 9 October disclosure – see paragraphs 26-30 above) and those details have now been incorporated into the most recent IC Code (see paragraph 109 above).

427. Consequently, the Court considers that there is now a basis in law for the requesting of intelligence from foreign intelligence agencies, and that that law is sufficiently accessible. Furthermore, the regime clearly pursues several legitimate aims, including the interests of national security, public safety and the economic well-being of the country, the prevention of disorder or crime, and the protection of the rights and freedoms of others. It therefore falls to the Court to assess the foreseeability and necessity of the regime. As already indicated, it will do so by examining whether the law meets the following requirements by indicating: the circumstances in which intercept material can be requested; the procedure to be followed for examining, using and storing the material obtained; the precautions to be taken when communicating the material obtained to other parties; and the circumstances in which the material obtained must be erased or destroyed (see the third to sixth safeguards referred to in paragraph 307 above).

(β) The circumstances in which intercept material can be requested

428. Chapter 12 of the IC Code (see paragraph 109 above) states that, save in exceptional circumstances, the intelligence services may only make a request to a foreign government for unanalysed intercepted communications and/or associated communications data if an interception warrant under RIPA has already been issued by the Secretary of State, the assistance of the foreign government is necessary to obtain the particular

communications because they cannot be obtained under the existing warrant, and it is necessary and proportionate for the intercepting agency to obtain those communications. A RIPA interception warrant means either a section 8(1) warrant in relation to the subject at issue; a section 8(4) warrant and an accompanying certificate which includes one or more “descriptions of intercepted material” covering the subject’s communications; or, where the subject is known to be within the British Islands, a section 8(4) warrant and an accompanying certificate which includes one or more “descriptions of intercepted material” covering his or her communications, together with an appropriate section 16(3) modification.

429. Where exceptional circumstances exist, a request for communications may be made in the absence of a relevant RIPA interception warrant only if it does not amount to a deliberate circumvention of RIPA or otherwise frustrate its objectives (for example, because it is not technically feasible to obtain the communications via RIPA interception), and it is necessary and proportionate for the intercepting agency to obtain those communications. In such a case the request must be considered and decided on by the Secretary of State personally, and, pursuant to the revised IC Code, notified to the Interception of Communications Commissioner (see paragraph 109 above). According to information disclosed during the *Liberty* proceedings, and confirmed in the Government’s submissions in the present case, no request for intercept material has ever been made in the absence of an existing RIPA warrant.

430. In light of the above considerations, the Court considers that the circumstances in which the respondent State may request interception or the conveyance of intercepted material are sufficiently circumscribed in domestic law to prevent the State from using this power to circumvent either domestic law or its Convention obligations.

(γ) Procedure to be followed for storing, accessing, examining and using the material obtained

431. By virtue of section 19(2) of the Counter-Terrorism Act 2008 (“CTA” – see paragraph 103), information obtained by any of the intelligence services in connection with the exercise of any of their functions may be used in connection with the exercise of any of their other functions. However, the intelligence services are data controllers for the purposes of the Data Protection Act 1998 and are required to comply with the data protection principles in Part 1 of Schedule 1 to the DPA. While compliance with these principles is subject to exemption by ministerial certificate, they cannot be exempted from the obligation to comply with the fifth and seventh data protection principles, which provide that personal data processed for any purpose shall not be kept for longer than is necessary for that purpose; and 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. A member of the intelligence services commits an offence under section 1(1) of the OSA (see paragraph 107 above) if he discloses, without lawful authority, any information relating to security or intelligence which is, or has been, in his possession by virtue of his position.

432. More specifically, Chapter 12 of the IC Code makes it clear that where intercepted communications content or communications data are obtained by the intelligence services from a foreign government in circumstances where the material identifies itself as the product of an interception, 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 intelligence services as a result of interception under RIPA (see paragraph 109 above). This means that the safeguards in section 15 and 16 of RIPA, as supplemented by Chapter 7 of the IC Code, apply equally to intercepted communications and communications data obtained from foreign governments.

433. The Court has already given careful consideration to the safeguards in section 15 and 16 of RIPA, as supplemented by Chapter 7 of the IC Code, in its assessment of the section 8(4) regime (see paragraphs 361-363 above). In brief, material obtained from foreign intelligence agencies must be stored securely and must not be accessible to persons without the required level of security clearance. Access by the analyst is limited to a defined period of time, and if renewed, the record must be updated giving reasons for renewal. Before being able to examine material obtained from foreign intelligence agencies, specially authorised and vetted analysts must make a record of why access to the material is necessary for one of the statutory purposes set out in section 5(3) of RIPA, and proportionate. They cannot select material for examination using criteria that refer to the communications of individuals known currently to be in the British Islands (unless there is a warrant with a section 16(3) modification, or if, in the absence of a warrant, the Secretary of State has personally considered and approved the examination of those communications by reference to such factors).

434. Although the IPT had, in the *Liberty* proceedings, expressed concern that the section 16(2)(a) and (b) safeguards (which prevent intercepted material being selected for examination by reference to an individual known to be in the British Islands) did not appear to apply to material obtained from foreign governments in the absence of a warrant, the IC Code has since been amended to address this concern. Paragraph 12.5 now expressly provides that if a request made in the absence of a warrant is approved by the Secretary of State other than in relation to specific selectors, any communications obtained must not be examined by the intelligence services 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 (see paragraph 110 above).

435. In light of the foregoing, the Court would accept that the provisions relating to the storing, accessing, examining and using such material are sufficiently clear.

(δ) Procedure to be followed for communicating the material obtained to other parties

436. As with material intercepted directly pursuant to a RIPA warrant (see paragraphs 365-367 above), disclosure of material obtained from foreign intelligence agencies must be limited to the minimum necessary for the “authorised purposes” mentioned in section 5(3) of RIPA. In addition, disclosure to persons who have not been appropriately vetted is prohibited and material may only be disclosed to a person whose duties, which must relate to one of the authorised purposes, are such that he or she needs to know about the material to carry out those duties. In the same way, only so much of the intercepted material may be disclosed as the recipient needs.

437. Section 19(3), (4) and (5) of the CTA further provide that information obtained by MI5 and MI6 for the purposes of any of their functions may be disclosed by them for the purpose of the proper discharge of their functions; in the interests of national security; for the purpose of the prevention or detection of serious crime; or for the purpose of any criminal proceedings. Information obtained by GCHQ may be disclosed by it for the purpose of the proper discharge of its functions or for the purpose of any criminal proceedings (see paragraphs 104-105 above).

438. Moreover, a member of the intelligence services commits an offence under section 1(1) of the OSA 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 (see paragraph 107 above).

439. In light of the foregoing, the Court would also accept that the provisions relating to the procedure to be followed for communicating the material obtained to other parties are sufficiently clear.

(ε) The circumstances in which the material obtained must be erased or destroyed

440. Section 15(3) of RIPA and paragraph 7.8 of the IC Code require that every copy (together with any extracts and summaries) be destroyed securely as soon as retention is no longer necessary for any of the section 5(3) purposes (see paragraphs 74 and 90 above).

(ζ) Supervision and remedies

441. In nearly every case either a section 8(1) or 8(4) warrant will be in place, meaning that the Secretary of State (and, following the coming into force of IPA 2016, a judicial commissioner) will have authorised the interception. In exceptional circumstances, when a warrant is not in place, the Secretary of State must personally consider and decide upon the request, and the Interception of Communications Commissioner (now the Investigatory Powers Commissioner) must be notified. Therefore, in every case where a request has been made the Secretary of State will have deemed the interception to be necessary and proportionate (in the Convention sense).

442. Further oversight of the intelligence sharing regime is provided by the ISC, a cross-party Committee of Members of Parliament which exercises wide powers. Following an extensive review, on 13 July 2013 the ISC published a report in which it concluded that allegations “that GCHQ circumvented UK law by using the NSA’s PRISM programme to access the content of private communications” were unfounded as GCHQ had complied with its statutory duties contained in the ISA (see paragraphs 148-150 above).

443. Additional oversight was afforded by the Interception of Communications Commissioner, who was independent from both Government and the intelligence services. He was under a duty by section 58(4) of RIPA to make an annual report to the Prime Minister regarding the carrying out of his functions, which had to be laid before Parliament. As already noted, the Interception of Communications Commissioner has now been replaced by the Investigatory Powers Commissioner. On 17 October 2017, in a reply to a question posed by, *inter alia*, Privacy International, the new Commissioner confirmed that, like his predecessor, he had the power to oversee the Government’s intelligence sharing agreements, and that he intended to use those powers actively to ensure effective oversight.

444. A final level of oversight is provided by the IPT, and its effectiveness was demonstrated in the *Liberty* proceedings by the fact that it was able to ensure disclosure of certain arrangements which have now been incorporated into the IC Code (see paragraph 109 above).

(η) Proportionality

445. The Court has always been acutely conscious of the difficulties faced by States in protecting their populations from terrorist violence, which constitutes, in itself, a grave threat to human rights (see, for example, *Lawless v. Ireland (no. 3)*, 1 July 1961, §§ 28–30, Series A no. 3; *Ireland v. the United Kingdom*, 18 January 1978, Series A no. 25; and *Öcalan v. Turkey* [GC], no. 46221/99, § 179, ECHR 2005-IV) and in recent years it has expressly acknowledged – in response to complaints invoking a wide

range of Convention Articles – the very real threat that Contracting States currently face on account of international terrorism (see, for example, *Chahal v. the United Kingdom*, 15 November 1996, § 79, *Reports of Judgments and Decisions* 1996-V; *A. and Others v. the United Kingdom* [GC], no. 3455/05, § 181, ECHR 2009; *A. v. the Netherlands*, no. 4900/06, § 143, 20 July 2010; *Trabelsi v. Belgium*, no. 140/10, § 117, ECHR 2014 (extracts); and *Othman (Abu Qatada) v. United Kingdom*, no. 8139/09, § 183, ECHR 2012).

446. Faced with such a threat, the Court has considered it legitimate for Contracting States to take a firm stand against those who contribute to terrorist acts (see *Othman*, cited above, § 183). Due to the nature of global terrorism, and in particular the complexity of global terror networks, the Court accepts that taking such a stand – and thus preventing the perpetration of violent acts endangering the lives of innocent people – requires a flow of information between the security services of many countries in all parts of the world. As, in the present case, this “information flow” was embedded into a legislative context providing considerable safeguards against abuse, the Court would accept that the resulting interference was kept to that which was “necessary in a democratic society”.

(θ) Conclusions

447. In light of the foregoing considerations, the Court considers that the domestic law, together with the clarifications brought by the amendment of the IC Code, indicate with sufficient clarity the procedure for requesting either interception or the conveyance of intercept material from foreign intelligence agencies. In this regard, it observes that the high threshold recommended by the Venice Commission – namely, that the material transferred should only be able to be searched if all the material requirements of a national search were fulfilled and this was duly authorised in the same way as a search of bulk material obtained by the signals intelligence agency using its own techniques – is met by the respondent State’s regime. The Court further observes that there is no evidence of any significant shortcomings in the application and operation of the regime. On the contrary, following an investigation the ISC found no evidence whatsoever of abuse.

448. There has accordingly been no violation of Article 8 of the Convention.

(v) *Application of the test to material falling into the third category*

449. The third category of material identified at paragraph 417 above is material obtained by foreign intelligence agencies other than by the interception of communications. However, as the applicants have not specified the kind of material foreign intelligence agencies might obtain by methods other than interception they have not demonstrated that its

acquisition would interfere with their Article 8 rights. As such, the Court considers that there is no basis upon which it could find a violation of Article 8 of the Convention.

C. The Chapter II regime

450. The applicants in the second of the joined cases complained that the regime for the acquisition of communications data under Chapter II of RIPA was incompatible with their rights under Article 8 of the Convention.

1. Admissibility

451. In both their application to the Court and their initial observations, the applicants in the second of the joined cases incorrectly referred to the Chapter II regime as a regime for the interception of communications data. The Court observes, however, that it is not an interception regime, but rather permits certain public authorities to acquire communications data from Communications Service Providers (“CSPs”). In view of the “fundamental legal misunderstanding” upon which the complaint was originally founded, the Government submitted that the applicants have put forward no factual basis whatsoever for concluding that their communications were acquired in this way, and that they did not contend that they had been affected, either directly or indirectly, by the regime. The Government further argued that neither of the two conditions identified by the Court in *Roman Zakharov* (cited above, § 171) were satisfied in respect of the Chapter II regime: the applicants did not belong to a group “targeted” by the contested legislation, and they had available to them an effective domestic remedy. Consequently, they could not claim to be victims of the alleged violation within the meaning of Article 34 of the Convention.

452. The applicants, on the other hand, submitted that they were entitled to bring the present complaint since they could possibly have been affected by the impugned legislation and no effective remedy was available at the domestic level.

453. In assessing victim status the Court is predominantly concerned with whether an effective remedy existed which permitted a person who suspected that he or she was subject to secret surveillance to challenge that surveillance (see *Roman Zakharov*, cited above, § 171). In the present case, although the Court accepted that there existed special circumstances absolving the applicants from the requirement that they first bring their complaints to the IPT (see paragraph 268 above), it nevertheless found that the IPT was an effective remedy, available in theory and practice, which was capable of offering redress to applicants complaining of both specific incidences of surveillance and the general Convention compliance of surveillance regimes (see paragraphs 250-266 above). Consequently, the applicants can only claim to be “victims” on account of the mere existence

of the Chapter II regime if they are able to show that, due to their personal situation, they were potentially at risk of having their communications data obtained by the United Kingdom authorities through a request to a CSP (see *Roman Zakharov*, cited above, § 171).

454. In this regard, the Court notes that the Chapter II regime is not a regime for the bulk acquisition of communications data; rather, as stated previously, it permits public authorities to request specific communications data. Nevertheless, a large number of public authorities are entitled to make such requests, and the grounds on which a request might be made are relatively wide. Given that the applicants in the second of the joined cases are investigative journalists who have reported on issues such as CIA torture, counterterrorism, drone warfare, and the Iraq war logs, the Court would accept that they were potentially at risk of having their communications obtained by the United Kingdom authorities either directly, through a request to a CSP for their communications data, or indirectly, through a request to a CSP for the communications data of a person or organisation they had been in contact with.

455. The Court would therefore accept that they were “victims” within the meaning of Article 34 of the Convention. As this complaint is not inadmissible on any other grounds, it must be declared admissible.

2. *Merits*

(a) **The parties’ submissions**

(i) *The applicants*

456. The applicants submitted that Chapter II of RIPA permitted the obtaining of communications data in a wide range of ill-defined circumstances, without proper safeguards. In particular, they submitted that the legal framework and attendant safeguards were informed by a fundamental but erroneous premise; namely, that the obtaining of communications data was necessarily less intrusive than the interception of content. In particular, the applicants complained that in most cases authorisation for the acquisition of communications data was provided by a designated person, who was not sufficiently independent of the executive or even of the agency requesting the disclosure.

457. Furthermore, they complained that Chapter II provided few limitations as to the basis on which communications data could be acquired, since section 22 of RIPA allowed a designated person to authorise the acquisition of communications data on a broad range of grounds, provided that he or she believed it “necessary”. Finally, they argued that there were very few safeguards in respect of the handling and exploitation of communications data.

168 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

(ii) *The Government*

458. The Government pointed out that as the Chapter II regime was a targeted regime, there was nothing “unintentional” about its operation. On the contrary, the acquisition of communications data under it would always be intentional. It was therefore to be distinguished from regimes for the bulk interception or bulk acquisition of data.

459. The Government further argued that the amended Acquisition and Disclosure of Communications Data Code of Practice (“the ACD Code”) provided adequate safeguards in respect of the retention of communications data acquired under the Chapter II regime, and that the Interception of Communications Commissioner provided an important degree of oversight of the operation of the regime.

(b) **The Court’s assessment**

(i) *Existing case-law on the acquisition of communications data*

460. To date, the Court has only twice been called on to consider the Convention compliance of a regime for the acquisition by a public authority of communications data from a CSP: in *Malone* and, more recently, in *Ben Faiza* (both cited above). In *Malone*, the authorities had obtained the numbers dialled on a particular telephone and the time and duration of the calls from the Post Office, which, as the supplier of the telephone service, had acquired this data legitimately by a process known as “metering”. While the Court accepted that the use of the data could give rise to an issue under Article 8 of the Convention, it considered that “by its nature” it had to be distinguished from the interception of communications, which was “undesirable and illegitimate in a democratic society unless justified” (see *Malone*, cited above, § 84). However, it was not necessary for the Court to consider this issue in any further detail, since, in the absence of any legal framework governing the acquisition of records from the Post Office, the Court found that the interference had no basis in domestic law (see *Malone*, cited above, § 87).

461. While *Malone* is now thirty-four years old, the *Ben Faiza* judgment was delivered in February 2018. In that case the Court was considering an order issued to a mobile telephone operator to provide lists of incoming and outgoing calls on four mobile telephones, together with the list of cell towers “pinged” by those telephones. Pursuant to the domestic law in question (Article 77-1-1 of the Criminal Procedure Code), prosecutors or investigators could, on the authorisation of the former, require establishments, organisations, persons, institutions and administrations to provide them with documents in their possession which were required for the purposes of the investigation. The Court accepted that the measure was “in accordance with the law”, and that the law provided adequate safeguards against arbitrariness. In respect of those safeguards, the Court observed that

a request under Article 77-1-1 was subject to the prior authorisation of the public prosecutor's office; this obligation could not be derogated from under penalty of nullity of the act; and the legality of such a measure could be reviewed in subsequent criminal proceedings against the person concerned and, if found to be unlawful, the criminal courts could exclude the evidence so obtained (*Ben Faiza*, cited above, §§ 72-73).

462. In adopting this approach, the Court distinguished between methods of investigation which made it possible to identify the past geographical position of a person and those which made it possible to geolocate him or her in real time, indicating that the latter was more likely to violate the right to respect for private life. Consequently, in the view of the Court, the transmission to a judicial authority of existing data held by a public or private body was to be distinguished from the establishment of a surveillance system, such as the ongoing monitoring of a telephone line or the placing of a tracking device on a vehicle (*Ben Faiza*, cited above, § 74; see also paragraph 350 above).

463. The Court of Justice of the European Union has also addressed this issue. In *Digital Rights Ireland v. Minister for Communications, Marine and Natural Resources and Others and Settinger and Others* (Cases C-293/12 and C-594/12), the CJEU considered the validity of the Data Retention Directive, and in *Secretary of State for the Home Department v. Watson and Others* (C-698/15), the validity of domestic legislation containing the same provisions as that directive (see paragraphs 224-234 above). While its focus was on the retention of data by CSPs, it also considered the question of access to retained data by the national authorities. In doing so, it indicated that access should be limited to what was strictly necessary for the objective pursued and, where that objective was fighting crime, it should be restricted to fighting serious crime. It further suggested that access should be subject to prior review by a court or independent administrative authority, and that there should be a requirement that the data concerned be retained within the European Union. In light of the CJEU's findings, Liberty sought to challenge Part 4 of the IPA, which included a power to issue "retention notices" to telecommunications operators requiring the retention of data. In response, the Government conceded that Part 4 was incompatible with fundamental rights in EU law since access to retained data was not limited to the purpose of combating "serious crime"; and access to retained data was not subject to prior review by a court or an independent administrative body. The High Court held that the legislation had to be amended by 1 November 2018 (see paragraph 196 above).

(ii) *The approach to be taken in the present case*

464. The appropriate test in the present case will therefore be whether the Chapter II regime was in accordance with the law; whether it pursued a legitimate aim; and whether it was necessary in a democratic society, having

170 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

particular regard to the question of whether it provided adequate safeguards against arbitrariness.

(iii) *Examination of the Chapter II regime*

465. No interference can be considered to be “in accordance with law” unless the decision occasioning it complies with the relevant domestic law. It is in the first place for the national authorities, notably the courts, to interpret and apply the domestic law: the national authorities are, in the nature of things, particularly qualified to settle issues arising in this connection. The Court cannot question the national courts’ interpretation, except in the event of flagrant non-observance or arbitrariness in the application of the domestic legislation in question (see *Mustafa Sezgin Tanriku*, cited above, § 53; see also, *mutatis mutandis*, *Weber and Saravia*, cited above, § 90).

466. The Court observes that the Chapter II regime has a clear basis in both section 22 of RIPA and the ACD Code. However, as a Member State of the European Union, the Community legal order is integrated into that of the United Kingdom and, where there is a conflict between domestic and law and EU law, the latter has primacy. Consequently, the Government have conceded that Part 4 of the IPA is incompatible with EU law because access to retained data was not limited to the purpose of combating “serious crime”; and access to retained data was not subject to prior review by a court or an independent administrative body. Following this concession, the High Court ordered that the relevant provisions of the IPA should be amended by 1 November 2018 (see paragraph 196 above).

467. It is therefore clear that domestic law, as interpreted by the domestic authorities in light of the recent judgments of the CJEU, requires that any regime permitting the authorities to access data retained by CSPs limits access to the purpose of combating “serious crime”, and that access be subject to prior review by a court or independent administrative body. As the Chapter II regime permits access to retained data for the purpose of combating crime (rather than “serious crime”) and, save for where access is sought for the purpose of determining a journalist’s source, it is not subject to prior review by a court or independent administrative body, it cannot be in accordance with the law within the meaning of Article 8 of the Convention.

468. Accordingly, the Court finds that there has been a violation of Article 8 of the Convention.

III. ALLEGED VIOLATION OF ARTICLE 10 OF THE CONVENTION

469. The applicants in the third of the joined cases complained under Article 10 of the Convention about the section 8(4) regime and the intelligence sharing regime, arguing, in particular, that the protection

afforded by Article 10 was of critical importance to them as NGOs involved in matters of public interest, who were exercising a role of public watchdog of similar importance to that of the press; and the applicants in the second of the joined cases, being a journalist and newsgathering organisation, complained under Article 10 of the Convention about both the section 8(4) regime and the Chapter II regime.

470. Article 10 of the Convention provides as follows:

“1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.”

A. Admissibility

1. *The applicants in the third of the joined cases*

471. The Court has already found that as a general rule the IPT has shown itself to be a remedy, available in theory and practice, which is capable of offering redress to applicants complaining about both specific incidences of surveillance and the general Convention compliance of a surveillance regime (see paragraphs 250-266 above). The Court has, however, accepted that there existed special circumstances absolving the applicants in the first and second of the joined cases from the requirement that they exhaust this remedy (see paragraph 268 above), but as the applicants in the third of the joined cases challenged the Convention compliance of both the section 8(4) regime and the intelligence sharing regime before the IPT, they cannot benefit from the “absolution” afforded to the other applicants. Therefore, as they did not complain before the IPT that the intelligence sharing regime was incompatible with Article 10 of the Convention, this complaint must be declared inadmissible for failure to domestic remedies within the meaning of Article 35 § 1 of the Convention.

472. Furthermore, although these applicants did complain before the IPT that the section 8(4) regime was not compatible with Article 10, in doing so they primarily relied on the same arguments invoked in respect of their Article 8 complaint. Insofar as they sought to argue that Article 10 could apply to their investigatory activities as NGOs, this argument was only raised on 17 November 2014 (the first and second open hearings having taken place in July and October 2014). As the IPT considered that this

argument could have been raised at any time, in its judgment it had been raised far too late to be incorporated into the ambit of the *Liberty* proceedings (see paragraph 47 above).

473. Therefore, with regard to the Article 8(4) complaint, the Court finds that insofar as the applicants in the third of the joined cases seek to rely on the special protection afforded by Article 10 of the Convention to journalists, they have not exhausted domestic remedies within the meaning of Article 35 § 1 of the Convention. Their complaints under this head must also be declared inadmissible.

474. Finally, the Court considers that the more general Article 10 complaint – which the applicants raised before the IPT in good time – gives rise to no separate argument over and above that arising out of Article 8 of the Convention. It is not, therefore, necessary to examine this complaint.

2. The applicants in the second of the joined cases

475. As the Court has acknowledged that the applicants in the second of the joined cases were, exceptionally, absolved from the requirement that they first bring their complaints to the IPT, they cannot be said to have failed to exhaust domestic remedies within the meaning of Article 35 § 1 of the Convention. As their complaints are not inadmissible on any other ground, they must, therefore, be declared admissible.

476. Moreover, the applicants in the second of the joined cases are a journalist and a newsgathering organisation, who complain about the interference with confidential journalistic material occasioned by the operation of both the section 8(4) regime and the Chapter II regime. As such, their complaints raise separate issues to those raised under Article 8 of the Convention, which will be examined below.

B. Merits

1. The parties' submissions

(a) The applicants

477. The applicants argued that as freedom of the press constituted one of the essential foundations of a democratic society, and the protection of journalistic sources was one of the cornerstones of freedom of the press, Article 10 of the Convention imposed additional and more exacting requirements where an interference gave rise to a significant risk of revealing journalistic sources or confidential journalistic material. In this regard, they submitted that surveillance measures which ran a significant risk of identifying journalistic source material had to be justified by an “overriding public interest” (*Sanoma Uitgevers B.V.*, cited above, §§ 51 and 90, 14 September 2010 and *Goodwin v. the United Kingdom*, 27 March

1996, § 39 *Reports of Judgments and Decisions* 1996-II); and authorisation could only be granted by a judge or other independent adjudicative body.

478. The applicants submitted that as journalists involved in matters of public interest, who were exercising a role of public watchdog, the protection afforded by Article 10 was of critical importance to them.

479. In respect of the section 8(4) regime, the applicants argued that the interception of material gathered through bulk surveillance was not attended by adequate safeguards. First of all, the definition of “confidential journalistic material” in the IC Code of Practice was too narrow, as it was limited to material acquired for the purpose of journalism and held subject to an undertaking to hold it in confidence. This definition was inconsistent with the Court’s broader definition (for example, in *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, no. 39315/06, § 86, 22 November 2012). Secondly, the regime did not comply with the strict requirements of Article 10 where surveillance measures might reveal journalistic source material (in the applicants’ submissions, the existence of an “overriding public interest” and judicial – or at least independent – authorisation).

480. With regard to the Chapter II regime, the applicants complained that the ACD Code failed to recognise that communications data could be privileged, and that the obtaining of communications data which constituted confidential journalistic material was as intrusive as obtaining content, since a single piece of communications data could reveal the identity of a journalist’s source, and when aggregated and subjected to modern data-mining technology, it could reveal an enormous range of (journalistically privileged) information. The applicants further complained that in most cases authorisation for the acquisition of communications data was provided by a designated person, who was not sufficiently independent of the executive, or even of the agency requesting the disclosure. While an additional safeguard now existed requiring that applications made in order to identify a journalist’s source be authorised by a judge, they did not apply where the identification of the source was incidental rather than intended.

(b) The Government

481. In the Government’s submissions, prior authorisation was the only respect in which the applicants contended that the position regarding the “in accordance with the law” test might differ under Article 10 from that under Article 8, and in respect of which they asserted that their identity as journalists might be material to the analysis. However, there was no authority in the Court’s case-law for the proposition that prior judicial (or independent) authorisation was required for a strategic monitoring regime by virtue of the fact that some journalistic material might be intercepted in the course of that regime’s operation. On the contrary, the Court had drawn a sharp and important distinction between the strategic monitoring of

communications and/or communications data, which might inadvertently “sweep up” some journalistic material, and measures that targeted journalistic material, particularly for the purposes of identifying sources, where prior authorisation would be required.

482. With regard to Chapter II of RIPA, the Government pointed out that pursuant to the amended Acquisition and Disclosure of Communications Data Code of Practice (“the ACD Code”), where the identification of a journalist’s source was intended, judicial authorisation was required. As there was nothing “unintentional” about the operation of the Chapter II regime, the acquisition of communications data under it would always be intentional and further safeguards were not required for the unintentional acquisition of material disclosing a journalist’s source.

483. The Government further argued that the ACD Code provided for the protection of confidential material, including journalistic material. Such material should only be retained where necessary and proportionate for one of the authorised purposes in section 15(4) of RIPA; it must be destroyed securely when its retention was no longer needed for those purposes; and, if retained, there had to be adequate information management systems in place to ensure that retention remained necessary and proportionate. Where it was retained or disseminated to an outside body, reasonable steps had to be taken to mark it as confidential, and where any doubt existed, legal advice had to be sought about its dissemination. Finally, any case where confidential material was retained had to be notified to the Commissioner as soon as reasonably practical and the material had to be made available to the Commissioner on request.

2. The submissions of the third parties

(a) The Helsinki Foundation for Human Rights

484. The Helsinki Foundation submitted that the protection of journalistic sources was undermined not only by the surveillance of the content of journalists’ communications, but also by the surveillance of related metadata which could, by itself, allow for the identification of sources and informants. It was especially problematic that confidential information could be acquired without the journalists’ knowledge or control, thereby depriving them of their right to invoke confidentiality, and the ability of their sources to rely on guarantees of confidentiality.

(b) The National Union of Journalists (“NUJ”) and the International Federation of Journalists (“IFJ”)

485. The NUJ and the IFJ submitted that the confidentiality of sources was indispensable for press freedom. They also expressed concern about the possible sharing of data retained by the United Kingdom with other countries. If confidential journalistic material were to be shared with a

country which could not be trusted to handle it securely, it could end up in the hands of people who would harm the journalist or his or her source. In the interveners' view, the safeguards in the updated IC and ACD Codes of Practice were not adequate, especially where the journalist or the identification of his or her source was not the target of the surveillance measure.

(c) The Media Lawyers' Association ("MLA")

486. The MLA expressed deep concern that domestic law was moving away from the strong presumption that journalistic sources would be afforded special legal protection, since surveillance regimes allowed the authorities to intercept journalists' communications without the need for prior judicial authorisation. Since the protection of journalists' sources was one of the core components of Article 10, more robust protection was required.

3. The Court's assessment

(a) General principles

487. The Court reiterates that freedom of expression constitutes one of the essential foundations of a democratic society and that the safeguards to be afforded to the press are of particular importance. The protection of journalistic sources is one of the cornerstones of freedom of the press. Without such protection, sources may be deterred from assisting the press in informing the public about 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 (see, *inter alia*, *Sanoma Uitgevers B.V.*, cited above, § 50; *Weber and Saravia*, cited above, § 143; *Goodwin*, cited above, § 39; and *Roemen and Schmit v. Luxembourg*, no. 51772/99, § 46, ECHR 2003-IV).

488. The Court has always subjected the safeguards for respect of freedom of expression in cases under Article 10 of the Convention to special scrutiny. Having regard to the importance of the protection of journalistic sources for press freedom in a democratic society, an interference cannot be compatible with Article 10 of the Convention unless it is justified by an overriding requirement in the public interest (*Sanoma Uitgevers B.V.*, cited above, § 51; *Goodwin*, cited above, § 39; *Roemen and Schmit*, cited above, § 46; and *Voskuil v. the Netherlands*, no. 64752/01, § 65, 22 November 2007).

489. The Court has recognised that there is "a fundamental difference" between the authorities ordering a journalist to reveal the identity of his or her sources, and the authorities carrying out searches at a journalist's home and workplace with a view to uncovering his or her sources (compare *Goodwin*, cited above, with *Roemen and Schmit*, cited above, § 57). The

Court considered that the latter, even if unproductive, constituted a more drastic measure than an order to divulge the source's identity, since investigators who raid a journalist's workplace have access to all the documentation held by the journalist (*Roemen and Schmit*, cited above, § 57). However, the Court has also drawn a distinction between searches carried out on journalists' homes and workplaces "with a view to uncovering their sources", and searches carried out for other reasons, such as the obtaining of evidence of an offence committed by a person other than in his or her capacity as a journalist (*Roemen and Schmit*, cited above, § 52). Similarly, in *Weber and Saravia*, the only case in which the Court has considered, *in abstracto*, the Article 10 compliance of a secret surveillance regime on account of the potential for interference with confidential journalistic material, it considered it decisive that the surveillance measures were not aimed at monitoring journalists or uncovering journalistic sources. As such, it found that the interference with freedom of expression could not be characterised as particularly serious (*Weber and Saravia*, cited above, § 151).

(b) The application of the general principles to the present case

(i) The section 8(4) regime

490. With regard to the question of victim status, the Court recalls that in *Weber and Saravia* it expressly recognised that the impugned surveillance regime had interfered with the first applicant's freedom of expression as a journalist (*Weber and Saravia*, cited above, §§ 143-145). In the present case, the applicants in the second of the joined cases are journalists and can similarly claim to be "victims" of an interference with their Article 10 rights by virtue of the operation of the section 8(4) regime.

491. For the reasons set out in respect of the Article 8 complaint, the Court considers that – save for its concerns about the oversight of the selection process and the safeguards applicable to the selection of related communications data (see paragraph 387 above) – the section 8(4) regime was in accordance with the law (see paragraphs 387-388 above). Furthermore, it pursued the legitimate aims of protecting interests of national security, territorial integrity and public safety, and preventing disorder and crime.

492. With regard to "necessity", the Court reiterates that, having regard to the importance of the protection of journalistic sources for the freedom of the press in a democratic society, an interference could not be compatible with Article 10 of the Convention unless it was justified by an overriding requirement in the public interest (*Weber and Saravia*, cited above, § 149). In this regard, it notes that the surveillance measures under the section 8(4) regime – like those under the G10 Act which were considered in *Weber and Saravia* – are not aimed at monitoring journalists or uncovering journalistic

sources. Generally the authorities would only know when examining the intercepted communications if a journalist's communications had been intercepted. Consequently, it confirms that the interception of such communications could not, by itself, be characterised as a particularly serious interference with freedom of expression (*Weber and Saravia*, cited above, § 151). However, the interference will be greater should these communications be selected for examination and, in the Court's view, will only be "justified by an overriding requirement in the public interest" if accompanied by sufficient safeguards relating both to the circumstances in which they may be selected intentionally for examination, and to the protection of confidentiality where they have been selected, either intentionally or otherwise, for examination.

493. In this regard, paragraphs 4.1 – 4.8 of the IC Code require special consideration to be given to the interception of communications that involve confidential journalistic material and confidential personal information (see paragraph 90 above). However, these provisions appear to relate solely to the decision to issue an interception warrant. Therefore, while they might provide adequate safeguards in respect of a targeted warrant under section 8(1) of RIPA, they do not appear to have any meaning in relation to a bulk interception regime. Furthermore, the Court has already criticised the lack of transparency and oversight of the criteria for searching and selecting communications for examination (see paragraphs 339, 340, 345 and 387 above). In the Article 10 context, it is of particular concern that there are no requirements – at least, no "above the waterline" requirements – either circumscribing the intelligence services' power to search for confidential journalistic or other material (for example, by using a journalist's email address as a selector), or requiring analysts, in selecting material for examination, to give any particular consideration to whether such material is or may be involved. Consequently, it would appear that analysts could search and examine without restriction both the content and the related communications data of these intercepted communications.

494. Safeguards do exist in respect of the storing of confidential material once identified. For example, paragraph 4.29 of the IC Code (see paragraph 90 above) provides that such material should only be retained where it is necessary and proportionate for one of the authorised purposes in section 15(4) of RIPA, and it must be destroyed securely when it is no longer needed for one of these purposes. Furthermore, according to paragraph 4.30, if it is retained or disseminated to an outside body, reasonable steps should be taken to mark the information as confidential; and paragraph 4.31 requires that the Interception of Communications Commissioner be notified of the retention of such material as soon as reasonably practicable, and such material should be made available to him on request.

495. Nevertheless, in view of the potential chilling effect that any perceived interference with the confidentiality of their communications and, in particular, their sources might have on the freedom of the press and, in the absence of any “above the waterline” arrangements limiting the intelligence services’ ability to search and examine such material other than where “it is justified by an overriding requirement in the public interest”, the Court finds that there has also been a violation of Article 10 of the Convention.

(ii) *The Chapter II regime*

496. The applicants in the second of the joined cases also complained under Article 10 of the Convention about the regime for the acquisition of communications data from CSPs.

497. In considering the applicants’ Article 8 complaint, the Court concluded that the Chapter II regime was not in accordance with the law as it permitted access to retained data for the purpose of combating crime (rather than “serious crime”) and, save for where access was sought for the purpose of determining a journalist’s source, it was not subject to prior review by a court or independent administrative body (see paragraph 467 above).

498. The Court acknowledges that the Chapter II regime affords enhanced protection where data is sought for the purpose of identifying a journalist’s source. In particular, paragraph 3.77 of the ACD Code provides that where an application is intended to determine the source of journalistic information, there must be an overriding requirement in the public interest, and such applications must use the procedures of the Police and Criminal Evidence Act 1984 (“PACE”) to apply to a court for a production order to obtain this data (see paragraph 117 above). Pursuant to Schedule 1 to PACE, an application for a production order is made to a judge and, where the application relates to material that consists of or includes journalistic material, the application should be made *inter partes* (see paragraph 121 above). The internal authorisation process may only be used if there is believed to be an immediate threat of loss of human life, and that person’s life might be endangered by the delay inherent in the process of judicial authorisation (paragraphs 3.76 and 3.78-3.84 of the ACD Code – see paragraph 117 above).

499. Nevertheless, these provisions only apply where the purpose of the application is to determine a source; they do not, therefore, apply in every case where there is a request for the communications data of a journalist, or where such collateral intrusion is likely. Furthermore, in cases concerning access to a journalist’s communications data there are no special provisions restricting access to the purpose of combating “serious crime”. Consequently, the Court considers that the regime cannot be “in accordance with the law” for the purpose of the Article 10 complaint.

(iii) Overall conclusion

500. In respect of the complaints under Article 10 of the Convention, the Court therefore finds a violation in respect of the section 8(4) regime and the Chapter II regime.

IV. ALLEGED VIOLATION OF ARTICLE 6 OF THE CONVENTION

501. The applicants in the third of the joined cases further complained under Article 6 of the Convention that the limitations inherent in the IPT proceedings were disproportionate and impaired the very essence of their right to a fair trial.

502. Article 6 provides, as relevant:

“1. In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice.”

503. In particular, the applicants contended that there was a lack of independence and impartiality on the part of the IPT, evidenced by the fact that in November 2007 there had been a secret meeting between it and the Security Services which, they alleged, resulted in the adoption of a protocol pursuant to which MI5 agreed not to search or disclose any bulk data holdings relating to complainants; that they were not effectively represented in the closed proceedings; that the IPT failed to require the defendants to disclose key internal guidance; and that, following the hearing, the IPT had made its determination in favour of the wrong party.

504. The Government submitted that Article 6 of the Convention did not apply to surveillance proceedings, since the Commission and the Court had consistently held that decisions authorising surveillance did not involve the determination of “civil rights and obligations” within the meaning of Article 6 § 1. They further contended that even if Article 6 did apply, when the proceedings were taken as a whole the applicants could not be said to have been denied the right to a fair trial. In particular, they observed that the applicants did not have to overcome any evidential burden to apply to the IPT; there was scrutiny of all the relevant material, open and closed, by the IPT, which had full powers to obtain any material it considered necessary; material was only withheld where the IPT was satisfied that there were appropriate public interest and national security reasons for doing so; and finally, the IPT appointed Counsel to the Tribunal who in practice performed a similar function to that of a Special Advocate in closed material proceedings. With regard to the meeting in 2007 between MI5 and the IPT,

they advised the Court that at the meeting MI5 had indicated that, for the purposes of IPT proceedings, it would not routinely conduct searches of “reference data-bases”, being databases containing information about the population generally (such as the Voter’s Roll or telephone directories), for any mention of a complainant’s name; instead, such searches would only be carried out if the data was “relevant or had been relied on in the course of an investigation”.

505. In their third party intervention, the ENNHRI submitted that the principle of equality of arms – being a core aspect of Article 6 of the Convention – was incompatible with the exclusion of one party from a hearing in which the other participates, other than in exceptional circumstances where adequate procedural safeguards provide protection from unfairness and no disadvantage ensues.

506. To date, neither the Commission nor the Court has found that Article 6 § 1 of the Convention applies to proceedings relating to a decision to place a person under surveillance. For example, in *Klass v. Germany* the Commission found that Article 6 § 1 was not applicable either under its civil or under its criminal limb (see *Klass and Others*, cited above, §§ 57-61) and, more recently, in *Association for European Integration and Human Rights and Ekimdzhiev* (cited above, § 106) the Court “did not perceive anything in the circumstances of the case that could alter that conclusion”.

507. However, the IPT has itself gone further than this Court. In its joint Ruling on Preliminary Issues of Law in the *British-Irish Rights Watch Case*, it accepted that Article 6 applied to “a person’s claims under section 65(2)(a) and to his complaints under section 65(2)(b) of RIPA, as each of them involves “the determination of his civil rights’ by the Tribunal within the meaning of Article 6(1)” (see paragraph 137 above). Consequently, when the matter came before the Court in *Kennedy* it did not consider it necessary to reach a conclusion on the matter, since it held that, even assuming that Article 6 § 1 applied to the proceedings in question, there had been no violation of that Article (*Kennedy*, cited above, §§ 177-179 and §§ 184-191).

508. In the present case, it is similarly unnecessary for the Court to reach any firm conclusion on the question of the applicability of Article 6 of the Convention since, for the reasons set out below, it considers that the applicants’ complaint is manifestly ill-founded.

509. With regard to the applicants’ general complaints concerning the procedure before the IPT, including the limitations on disclosure and the holding of public hearings in the interests of national security, the Court recalls that similar complaints were made in *Kennedy* and the Court, having considered the relevant procedural rules, concluded that 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 restrictions on the applicant’s procedural rights were both

necessary and proportionate and did not impair the very essence of his Article 6 rights (*Kennedy*, cited above, §§ 177-179 and §§ 184-191).

510. The Court sees no reason to come to a different conclusion in the present case. It has already found, in paragraphs 250-265 above, that in view of the IPT's extensive power to consider complaints concerning the wrongful interference with communications pursuant to RIPA, it was an effective remedy, available in theory and practice, which was capable of offering redress to persons complaining of both specific incidences of surveillance and the general Convention compliance of a surveillance regime. Furthermore, these extensive powers were employed in the applicants' case to ensure the fairness of the proceedings; in particular, there was scrutiny of all the relevant material, open and closed, by the IPT; material was only withheld from the applicants where the IPT was satisfied that there were appropriate public interest and national security reasons for doing so; and finally, the IPT appointed Counsel to the Tribunal to make submissions on behalf of the applicants in the closed proceedings.

511. Insofar as the applicants complain about the meeting between the IPT and the intelligence services in 2007, the Court considers that, in view of the IPT's specialist role, the fact that its members met with the services to discuss procedural matters does not, of itself, call into question its independence and impartiality. Furthermore, the applicants have not adequately explained how the 2007 meeting impacted on the fairness of their IPT proceedings in 2014 and 2015. Although the applicants appear to suggest that the resulting protocol might have affected the IPT's ability to access information held about them, the Government's explanation of the protocol (namely, that it concerned an agreement not to conduct searches of databases containing information about the population generally, such as the Voter's Roll or telephone directories, unless the data was "relevant or had been relied on in the course of an investigation") confirms that it could have had no impact on the fairness of the IPT proceedings in the present case.

512. Finally, it would appear that the error regarding the identity of the applicants whose rights were violated was an administrative mistake (see paragraph 53 above) and, as such, does not indicate any lack of rigour in the judicial process.

513. Accordingly, the Court considers that the complaint under Article 6 § 1 of the Convention must be rejected as manifestly ill-founded pursuant to Article 35 § 3 (a) of the Convention.

V. ALLEGED VIOLATION OF ARTICLE 14 OF THE CONVENTION COMBINED WITH ARTICLES 8 AND 10 OF THE CONVENTION

514. The applicants in the third of the joined cases further complained under Article 14 of the Convention, read together with Articles 8 and 10, that the section 8(4) regime was indirectly discriminatory on grounds of

nationality because persons outside the United Kingdom were disproportionately likely to have their private communications intercepted; and section 16 of RIPA provides additional safeguards only to persons known to be in the British Islands.

515. Article 14 provides as follows:

“The enjoyment of the rights and freedoms set forth in [the] Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.”

516. However, the applicants have not substantiated their claim that persons outside the United Kingdom are disproportionately likely to have their private communications intercepted under the section 8(4) regime. First of all, although the regime targets “external communications”, this is defined as “a communication sent or received outside the British Islands”. This does not, therefore, exclude the interception of communications where one of the parties is in the British Islands. Secondly, and in any event, it has already been acknowledged that “internal communications” (where both the sender and receiver are in the British Islands) are frequently – and lawfully – intercepted as a by-catch of a section 8 (4) warrant.

517. Insofar as section 16 prevents intercepted material from being selected for examination according to a factor “referable to an individual who is known to be for the time being in the British Islands”, any resulting difference in treatment would not be based directly on nationality or national origin, but rather on geographical location. In *Magee v. the United Kingdom*, no. 28135/95, § 50, ECHR 2000-VI the Court held that as such a difference in treatment could not be explained in terms of personal characteristics, it was not a relevant difference in treatment for the purposes of Article 14 of the Convention and did not amount to discriminatory treatment within the meaning of Article 14 of the Convention (see *Magee*, cited above, § 50).

518. In any event, the Court is of the view that any difference in treatment based on geographic location was justified. The Government have considerable powers and resources to investigate persons within the British Islands and do not have to resort to interception of their communications under a section 8(4) warrant. They do not, however, have the same powers to investigate persons outside of the British Islands.

519. Accordingly, the Court considers that the complaint under Article 14 of the Convention, read together with Articles 8 and 10, must be rejected as manifestly ill-founded pursuant to Article 35 § 3(a) of the Convention.

VI. APPLICATION OF ARTICLE 41 OF THE CONVENTION

520. Article 41 of the Convention provides:

“If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party.”

A. Damage

521. The applicants did not submit any claim in respect of pecuniary or non-pecuniary damage. Accordingly, the Court considers that there is no call to award them any sum on that account.

B. Costs and expenses

522. The applicants in the first and second of the joined cases made a claim for costs and expenses incurred before the Court. The applicants in the first of the joined cases claimed GBP 208,958.55 in respect of their costs and expenses; and the applicants in the second of the joined cases claimed GBP 45,127.89. The applicants in the third of the joined cases made no claim in respect of costs and expenses.

523. The Government did not comment on the sums claimed.

524. According to the Court’s case-law, an applicant is entitled to the reimbursement of costs and expenses only in so far as it has been shown that these have been actually and necessarily incurred and are reasonable as to quantum. In the present case, regard being had to the documents in its possession and the above criteria, the Court considers it reasonable to award the applicants in the first of the joined cases the sum of EUR 150,000 for the proceedings before the Court; and the applicants in the second of the joined cases the sum of EUR 35,000 for the proceedings before the Court.

C. Default interest

525. The Court considers it appropriate that the default interest rate should be based on the marginal lending rate of the European Central Bank, to which should be added three percentage points.

FOR THESE REASONS, THE COURT:

1. *Declares*, unanimously, the complaints made by the applicants in the third of the joined cases concerning Article 6, Article 10, insofar as the applicants rely on their status as NGOs, and Article 14 inadmissible;
2. *Declares*, unanimously, the remainder of the complaints made by the applicants in the third of the joined cases admissible;
3. *Declares*, by a majority, the complaints made by the applicants in the first and second of the joined cases admissible;
4. *Holds*, by five votes to two, that there has been a violation of Article 8 of the Convention in respect of the section 8(4) regime;
5. *Holds*, by six votes to one, that there has been a violation of Article 8 of the Convention in respect of the Chapter II regime,
6. *Holds*, by five votes to two, that there has been no violation of Article 8 of the Convention in respect of the intelligence sharing regime;
7. *Holds*, by six votes to one, that, insofar as it was raised by the applicants in the second of the joined cases, there has been a violation of Article 10 of the Convention in respect of the section 8(4) regime and the Chapter II regime;
8. *Holds*, unanimously, that there is no need to examine the remaining complaints made by the applicants in the third of the joined cases under Article 10 of the Convention;
9. *Holds*, by six votes to one,
 - (a) that the respondent State is to pay the applicants, within three months from the date on which the judgment becomes final in accordance with Article 44 § 2 of the Convention, the following amounts, to be converted into the currency of the respondent State at the rate applicable at the date of settlement:
 - (i) to the applicants in the first of the joined cases: EUR 150,000 (one hundred and fifty thousand euros), plus any tax that may be chargeable to the applicants, in respect of costs and expenses;
 - (ii) to the applicants in the second of the joined cases: EUR 35,000 (thirty-five thousand euros), plus any tax that may be chargeable to the applicants, in respect of costs and expenses;
 - (b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amounts at a

BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT 185

rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points; and

10. *Dismisses*, unanimously, the remainder of the applicants' claim for just satisfaction.

Done in English, and notified in writing on 13 September 2018, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Abel Campos
Registrar

Linos-Alexandre Sicilianos
President

In accordance with Article 45 § 2 of the Convention and Rule 74 § 2 of the Rules of Court, the following separate opinions are annexed to this judgment:

- (a) partly concurring, partly dissenting opinion of Judge Koskelo, joined by Judge Turković; and
- (b) joint partly dissenting and partly concurring opinion of Judges Pardalos and Eicke.

L.-A.S.
A.C.

186 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT

APPENDIX

List of Applicants

App. No.	Applicants
58170/13	Big Brother Watch
58170/13	English PEN
58170/13	Open Rights Group
58170/13	Dr Constanze Kurz
62322/14	Bureau of Investigative Journalism
62322/14	Alice Ross
24960/15	Amnesty International Limited
24960/15	Bytes For All
24960/15	The National Council for Civil Liberties (“Liberty”)
24960/15	Privacy International
24960/15	The American Civil Liberties Union
24960/15	The Canadian Civil Liberties Association
24960/15	The Egyptian Initiative For Personal Rights
24960/15	The Hungarian Civil Liberties Union
24960/15	The Irish Council For Civil Liberties Limited
24960/15	The Legal Resources Centre

**PARTLY CONCURRING, PARTLY DISSENTING OPINION
OF JUDGE KOSKELO, JOINED BY JUDGE TURKOVIĆ**

1. I have voted, and agree, with the majority as regards points 1 to 3 of the operative provisions of the judgment, which concern the admissibility of the complaints. I have also joined the majority in finding a violation of Article 8 in respect of both the section 8(4) regime and the Chapter II regime. As regards the section 8(4) regime, however, I am not able in all respects to subscribe to the reasons given by the majority. As far as the intelligence sharing regime is concerned, unlike the majority, I have voted for finding a violation of Article 8.

I. The RIPA section 8(4) regime

2. The present case concerns legislation providing for secret surveillance, by means of bulk interception, of electronic communications which qualify as “external” (for an understanding of the concept of “external” communications see paragraphs 69-71 of the judgment). It is important to note that this type of secret surveillance of communications is not limited to certain already known or identified targets but is aimed at the discovery of threats and hitherto unknown or unidentified targets which might be responsible for threats (see paragraph 284 of the judgment). The relevant threats are broadly framed and comprise threats to national security or to the economic well-being of the country as well as threats arising from serious crime (see §§ 57-59).

3. It is obvious that such an activity – an untargeted surveillance of external communications with a view to discovering and exploring a wide range of threats – by its very nature takes on a potentially vast scope, and involves enormous risks of abuse. The safeguards against those risks, and the standards which under the Convention should apply in this regard, therefore raise questions of the highest importance. I am not convinced, in the light of present-day circumstances, that reliance on the Court’s existing case-law provides an adequate approach to the kind of surveillance regimes like the one we are dealing with here. A more thorough reconsideration would be called for. I acknowledge that this would be a task for the Court’s Grand Chamber. I will only raise some concerns which, in my view, require attention in this regard.

(i) The context of earlier case-law

4. Apart from the recent Chamber judgment in *Centrum för Rättvisa v. Sweden* (no. 35252/08, 19 June 2018), which is not yet final, the Court’s case-law has not dealt with the present kind of surveillance but with regimes which, as a matter of either law or fact, have been narrower in scope. Furthermore, in the light of current developments, I consider that reliance

on the line of existing case-law is no longer an adequate basis for assessing the standards which under the Convention should govern this particular domain.

5. The Court's case-law on secret surveillance of communications essentially dates back to *Klass and Others v. Germany* (cited in the judgment) which was decided by the Plenary Court four decades ago, and the admissibility decision in *Weber and Saravia v. Germany* (also cited in the judgment), which concerned an amended version of the same German legislation and was decided twelve years ago, in response to a complaint lodged in the year 2000.

6. As the Court noted in *Klass and Others*, the German legislation then at issue (the G 10) laid down a series of limitative conditions which had to be satisfied before a surveillance measure could be imposed. Thus, the permissible restrictive measures were *confined to cases in which there were factual indications for suspecting a person of planning, committing or having committed certain serious criminal acts*; measures could only be ordered if the establishment of the facts by another method was without any prospect of success or considerably more difficult; even then, the surveillance could cover *only the specific suspect or his presumed "contact-persons"*. Thus, the Court observed, "*so-called exploratory or general surveillance [was] not permitted by the contested legislation*" (see *Klass and Others*, § 51).

7. In this regard, the RIPA section 8(4) regime which is at issue in the present case is different from that in *Klass and Others* in that the section 8(4) regime does encompass what the Court then referred to as "exploratory" surveillance and which in fact constitutes an essential and critical feature of this particular regime. Consequently, the scope and purpose of the surveillance regime now at issue is wider than that addressed in *Klass and Others*.

8. In *Weber and Saravia*, the complaint concerned a revised version, adopted in 1994, of the German G 10, whereby the scope of permissible surveillance was extended to cover the monitoring of international wireless telecommunications (see *Weber and Saravia*, § 88) in order to allow a "strategic surveillance" of such communications by means of catchwords. According to the Government's submissions in that case, at the relevant time merely some ten per cent of all telecommunications were conducted by wireless means, and thus potentially subject to monitoring. In practice, monitoring was restricted to a limited number of foreign countries. The telephone connections of the State's own (i.e. German) nationals living abroad could not be monitored directly. The identity of persons telecommunicating could only be uncovered in rare cases in which a catchword had been used (*ibid.*, § 110).

9. The surveillance regime at issue in *Weber and Saravia* covered international wireless communications traffic, i.e. traffic transmitted via

BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT - 189
SEPARATE OPINIONS

microwave or satellite, the latter operating through a survey of the downlink to Germany. Line-bound international communications were not subject to monitoring except where the risk of a war of aggression was concerned.

10. It is noteworthy that at the time of the surveillance regime which gave rise to the complaint in *Weber and Saravia*, strategic monitoring was mainly carried out on telephone, telex and fax communications. In those days, surveillance did not extend to email communications (see the judgment of the Federal Constitutional Court of 14 July 1999, 1BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95, Rn 230, according to which, at the time of the hearing of the case in 1999, an expansion of strategic monitoring to email communications was only being planned for the future). One significant feature of communications by email, apart from the fact that nowadays they are so common, is that the identity of both the sender and recipient is usually directly available. Furthermore, many currently used means of communication or access to information through the Internet were only at embryonic stages at the time of the domestic complaint in *Weber and Saravia*.

(ii) *The context of the present case*

11. My point with the remarks above is to draw attention to the factual environment against the background of which those earlier cases were adjudicated, and the dramatic changes that have occurred since. The applicants have indeed referred to the technological “sea change” which has taken place.

12. What is important to note in this regard is that the technological “sea change” has had a twofold impact. On the one hand, technological developments have advanced the means by which surveillance of communications can be carried out. On the other hand, new technologies have revolutionised the ways in which people communicate, access, use and share information. That change is deeper than just a matter of volume. The digital age has in some respects transformed people’s lifestyles.

13. As a result of these changes, the potential exposure nowadays of a vast range of communications and other online activities to secret surveillance is far greater than before. In the wake of such developments, the potential risks of abuse arising from such surveillance have increased as well. Thus, the factual context in which “exploratory” or “strategic” secret surveillance operates is dramatically different from the circumstances that still prevailed a couple of decades ago, when the *Weber and Saravia* application was lodged, let alone four decades ago, when *Klass and Others* was decided. In the light of such changes, it is problematic and troubling to approach the question of the necessary safeguards against abuse simply by applying standards that were considered sufficient under significantly or even essentially different factual circumstances.

190 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT -
SEPARATE OPINIONS

14. Furthermore, the “sea change” in terms of technologies and digitalised lifestyles is not the only development to be taken into consideration. The threats on account of which surveillance of communications is considered necessary have also changed. In this regard, too, the picture is twofold. On the one hand, for instance, there have been real and well-known aggravations in the risks of international terrorism. On the other, there is also increasing evidence of how various threats can be invoked, rightly or wrongly, in order to justify measures that entail restrictions on individual rights and freedoms. The notion of terrorism, for instance, may sometimes be used quite loosely and opportunistically in a desire to legitimise interferences with such rights and freedoms. Especially where secret surveillance is conducted in order to discover and explore broadly formulated threats such as those to national security or the nation’s economic well-being, the need for real safeguards through independent control and review is obvious.

15. There is yet another “sea change” calling for heightened attention in the assessment of the necessary standards in the context of secret surveillance of communications. It is the degradation of respect for democratic standards and the rule of law of which there is increasing evidence in a number of States. While I am not suggesting that the present respondent State is a case in point in this regard, the Convention standards must nevertheless be considered in the light of the fact that such developments testify to the actual or potential fragility of safeguards, institutional arrangements and the underlying assumptions that in ideal circumstances might appear adequate in order to minimise the risks of abuse. In fact, the same threats that are invoked to justify secret surveillance may also serve to reinforce tendencies toward a weakening of the checks and balances which underpin adherence to the rule of law and democratic governance.

(iii) Concerns

16. In line with the majority, I agree that the Contracting States must enjoy a wide margin of appreciation in determining whether the protection of national security requires the kind of surveillance of communications which is at issue in the present case (paragraph 314 of the present judgment). However, given the high risks of abuse, which at worst may undermine not only individual rights and freedoms but democracy and the rule of law more generally, the margin must be narrow when it comes to the necessary safeguards against abuse.

17. Under the impugned legislation, one of the striking features is that all of the supervisory powers entrusted to authorities with independence from the executive are of an *ex post* nature. Another striking feature is that not only are the general protective aims of the legislation very broadly framed, but also the specific authorisations (warrants and certificates) issued

BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT - 191
SEPARATE OPINIONS

by the Secretary of State appear to be formulated in very broad and general terms (see paragraphs 156 and 342). Furthermore, the concrete search and selection criteria which are applied to filter intercepted communications for reading of their content are determined by the analysts conducting the surveillance (see paragraphs 157, 340 and 345-46 of the present judgment). As indicated by the domestic findings, the latter are not even subject to any meaningful subsequent oversight by independent bodies (see paragraphs 157 and 340).

18. Ever since *Klass and Others*, the Court has indeed held that in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse (see *Klass and Others*, §§ 49-50). This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the 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 (*ibid.*, § 50).

19. As discussed above, in the light of the changes in both the nature and scope of surveillance and in the prevailing factual realities, the circumstances have indeed evolved in such a way and to such an extent that I find it difficult to accept that the adequacy of safeguards should nevertheless be assessed simply by relying on the case-law that has arisen under different legal and factual framework conditions.

20. In particular, given the present overall context, I question the approach according to which prior independent control by a judicial authority should not be a necessary requirement in the system of safeguards.

21. Already in *Klass and Others*, when considering the initial stage of control, the Court stated that, in a field where abuse was potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it was in principle desirable to entrust supervisory control to a judge (see *Klass and Others*, § 56). Under the G 10 legislation, judicial control was replaced by an initial control effected by an official qualified for judicial office and by the control provided by the Parliamentary Board and the G 10 Commission. In that case the Court concluded that, having regard to the nature of the supervisory and other safeguards provided for by the G 10, the exclusion of judicial control did not exceed the limits of what might be deemed necessary in a democratic society. The Court noted that the Parliamentary Board and the G 10 Commission were independent of the authorities carrying out the surveillance and vested with sufficient powers and competence to exercise an effective and continuous control. Furthermore, the democratic character was reflected in the balanced membership of the Parliamentary Board, on which the opposition was represented and was thus able to participate in the

control of the measures ordered by the competent Minister, who was accountable to the Bundestag. The Court found that the two supervisory bodies could, in the circumstances of the case, be regarded as enjoying sufficient independence to give an objective ruling (*ibid.*).

22. As indicated above, in my view the legal and factual circumstances of that case, which go back four decades, cannot be considered comparable to the situation now under consideration. It is somewhat striking that in *Weber*, despite the important changes in the legislative and factual framework, the Court succinctly stated that it saw no reason to reconsider the conclusion in *Klass and Others* (see *Weber and Saravia*, § 117). In any event, in the light of the circumstances prevailing at the present time, such reconsideration seems to me to be indispensable.

23. Where, as in the present case, the interception (as a matter of technical necessity) encompasses vast volumes of communications traffic in an indiscriminate manner, without being linked to any kind of prior elements of suspicion related to the threats by reason of which the surveillance is conducted, everything in terms of the protection of individuals and their rights depends on whether and how the subsequent stages of the treatment of the intercepted communications provide effective and reliable safeguards for those rights, and against any abuse of the surveillance. Under such circumstances, given the potential intrusiveness of the surveillance and the abundant risks of abuse, I consider that it cannot be appropriate that all the *ex ante* safeguards remain in the hands of the executive. I think the applicants are right to argue that there is a need for an “updating” of the standards as regards prior independent judicial authorisation. It seems to me to be important that the authorities of the executive branch should be required to explain and justify before an independent judicial authority the grounds on which a particular surveillance should be authorised, and to account for the search criteria on the basis of which the intercepted communications will be filtered and selected for a review of their content.

24. In this respect, I am not convinced by the arguments advanced by the majority in support of the position that prior judicial control is unnecessary (paragraphs 318-20). The majority acknowledge that judicial authorisation is not inherently incompatible with the effective functioning of bulk interception (paragraph 318). Indeed, the recent case of *Centrum för Rättvisa v. Sweden* (cited above) offers an illustration, as it deals with Swedish legislation under which prior judicial authorisation is required.

25. The main argument against imposing such a requirement appears to be that it would not entail a sufficient safeguard, and that even in the absence of prior judicial authorisation the existence of independent oversight by the IPT and the Interception of Communications Commissioner provide adequate safeguards against abuse. In my view, it is obvious that prior judicial authorisation cannot in itself be sufficient and

BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT - 193
SEPARATE OPINIONS

that further, robust safeguards such as those in place in the UK are indeed required. However, the fact that a given safeguard would not be sufficient is not enough to support a conclusion that it should not be considered necessary. In my opinion, it is quite essential to have in place an adequate system of safeguards, including controls exercised by independent bodies, both *ex ante* and *ex post*.

26. While the safeguards *ex post* that are provided for in the UK legislation and practice appear to set a good model in this domain, this does not in my view suffice to remedy the fact that the authorisation and implementation of the surveillance are wholly in the hands of the executive authorities, without any independent control *ex ante*. In this respect, the system of safeguards is even weaker than that considered by the Court in both *Klass and Others* and *Weber and Saravia*, in that under the German G 10 regime, although the surveillance was not subject to prior authorisation by a court, it had to be authorised by the G 10 Commission (see *Weber and Saravia*, cited above, § 115), which was not an executive branch body (*ibid.*, § 25). Moreover, according to the judgment of the Federal Constitutional Court of 14 July 1999 (cited above, Rn 87), a list of search concepts was part of each restriction order, whereas in the present case it has transpired that the search and selection criteria are determined by the analysts operating the surveillance and are not subject to any prior supervision, nor any meaningful subsequent oversight (see paragraphs 157, 340 and 345-46 of the present judgment).

27. In sum, what we have before us now is a regime of secret surveillance, the reach of which under the prevailing factual circumstances is unprecedented, and under which a very wide operational latitude is left to the services operating the surveillance, without any independent *ex ante* control or constraint, and under which the search and selection criteria are not even *ex post* subject to any robust independent control. I find such a situation highly problematic. An independent *ex ante* control is all the more important because of the secret nature of the surveillance, which in practice reduces the possibility that individuals will have recourse to the safeguards available *ex post*.

28. I also consider that the remarks made by the majority in paragraph 319 of the judgment are not capable of supporting a conclusion according to which prior independent judicial authorisation should not be required. Rather, the argument that even judicial scrutiny may fail its function serves to underline the crucial importance which attaches to the requirement that such control must have effective guarantees of independence, in order to meet the proper standards of the necessary safeguards.

29. In short, while I agree with the conclusions set out in paragraph 387 of the judgment, I do not consider those shortcomings to be the only ones that justify a finding of a violation of Article 8 in the present case. In

particular, taking into account the present legal and factual context, I do not believe that the necessary safeguards in the circumstances of surveillance based on the bulk interception of communications can be sufficient without including an independent *ex ante* judicial control. The position according to which prior judicial control of authorisations for secret surveillance of communications was a desirable but not a necessary safeguard stems from *Klass and Others* which, firstly, concerned a more limited surveillance regime than the one now at issue and did not permit “exploratory surveillance” at all, and which, secondly, was decided four decades ago against the backdrop of factual circumstances that in many relevant respects were different from those prevailing today. That position was later, in *Weber and Saravia*, carried over to a surveillance regime which did have more similarities with the RIPA section 8(4) regime but nevertheless operated in conditions very different from those prevailing in the modern digitalised societies. For the reasons outlined above, that position should, in my view, no longer be maintained by the Court.

II. The intelligence-sharing regime

30. It is easy to agree with the principle that any arrangement under which intelligence from intercepted communications is obtained via foreign intelligence services, whether on the basis of requests to carry out such interception or to convey its results, should not be allowed to entail a circumvention of the safeguards which must be in place for any surveillance by domestic authorities (see paragraphs 216, 423 and 447). Indeed, any other approach would be implausible.

31. On this basis I consider, in sum, that the shortcomings referred to above in the context of the section 8(4) regime also attach to the intelligence-sharing regime (see paragraphs 109 and 428-29). I therefore conclude that the safeguards have not been adequate and that there has been a violation of Article 8 in respect of this regime also.

JOINT PARTLY DISSENTING AND PARTLY
CONCURRING OPINION OF JUDGES PARDALOS AND
EICKE***Introduction***

1. For the reasons set out in more detail below, we are unfortunately, not able to agree with the majority in relation to two aspects of the judgment in this case; namely

(a) that the applicants in the first and second of the joined cases had shown “special circumstances absolving them from the requirement to exhaust” domestic remedies by first bringing proceedings before the IPT (§§ 266-268 and operative part § 3; “admissibility”); and

(b) that there has been a breach of Article 8 of the Convention in respect of the section 8(4) regime (§ 388 and operative part § 4; “the section 8(4) regime”).

2. In relation to the latter issue our position is reinforced by the contrast between the conclusions reached by the majority in this case and that reached in the judgment in *Centrum För Rättvisa v. Sweden*, no. 35252/08 (not yet final); a judgment adopted by the Third Section of this Court on 19 June 2018, a mere two weeks before the final deliberations in this case. In that case, the Court concluded, unanimously, that, despite having identified “some areas where there is scope for improvement” (§ 180) and “making an overall assessment and having regard to the margin of appreciation enjoyed by the national authorities in protecting national security” (§ 181), the Swedish system of signals intelligence provided adequate and sufficient guarantees against arbitrariness and the risk of abuse; as a consequence, it was held that the relevant legislation met the “quality of law” requirement, that the “interference” established could be considered as being “necessary in a democratic society” and that the structure and operation of the system were proportionate to the aim sought to be achieved.

3. That said, we agree both with:

(a) the underlying general principles identified by the Court both in this case and in *Centrum För Rättvisa* to be applied in relation to these aspects of the case; as well as

(b) the conclusion of the majority in this case that, for the reasons given in the judgment, there has been no breach of Article 8 of the Convention in relation to the intelligence sharing regime (§§ 447-448 and operative part § 6) and that there is no need to examine the remaining complaints made by the applicants in the third of the joined cases under Article 10 of the Convention.

4. In relation to the findings that there has been a breach of the Convention in relation to the Chapter II regime (§§ 468 and 500, operative part §§ 5 and 7) as well as the conclusions under Article 41 of the Convention (operative part § 9), one of us (Judge Pardalos) considered that her conclusion on the admissibility of the first and second of the joined cases invariably determined the related substantive issues against the applicants in those cases. By contrast, Judge Eicke considered that, the Court having decided that the first and second cases were, contrary to his view, admissible he was required, as a member of that Court, to go on and decide those cases on the merits by reference to the evidence and pleadings before the Court.

Admissibility

5. As indicated above, we agree with the majority that, for the reasons they give, the IPT is and has been an effective remedy “since Kennedy was decided in 2010” (§ 268); i.e. a remedy which is “available in theory and practice” and “capable of offering redress to applicants complaining of both specific incidences of surveillance and the general Convention compliance of surveillance regimes” (§ 265). Consequently, applicants before this Court will be expected to have exhausted this domestic remedy before the Court has jurisdiction to entertain their application under Article 35 § 1 of the Convention.

6. In addition to the purely legal point that, under Article 35 § 1, the Court “may only deal with the matter after all domestic remedies have been exhausted”, we would underline what the majority says in § 256 about the invaluable assistance derived by the Court, in examining a complaint before it, from the “elucidatory” role played by the domestic courts (in this case the IPT) both generally as well as in the specific context of considering the compliance of a secret surveillance regime with the Convention.

7. For the reasons set out below, however, we disagree with the conclusion reached by the majority (§ 268) that there existed, in this case, “special circumstances” absolving the applicants in the first and second of the joined cases from satisfying this requirement.

8. Firstly, as the majority implicitly accepts (§ 267), the case of *Kennedy* is clearly distinguishable on its facts from the present case. After all, the applicant in that case had already brought a specific complaint about the section 8(1) regime before the IPT before applying to this Court. Consequently, unlike the applicants in the first and second of these joined cases, Mr Kennedy was not inviting the Court to consider his general complaint entirely *in abstracto*. Furthermore, in its judgment in that case, the Court considered it “important” that his challenge was (consequently) exclusively a challenge to primary legislation. By contrast, in the present cases the scope of each of the regimes complained of (bulk interception,

BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT – 197
SEPARATE OPINIONS

intelligence sharing and the acquisition of communications data) is significantly broader than that of the section 8(1) regime, and the applicants' complaints concern not only primary legislation, but the overall legal framework governing those regimes (including the alleged absence of any relevant arrangements or other safeguards). Consideration of the broader legal framework necessarily requires an examination of both RIPA and the relevant Codes of Practice, together with any "below the waterline" arrangements and/or safeguards. In view of the much broader scope of both their complaints and the impugned regimes, none of which had been the subject of any examination by the IPT, it should have been evident to the applicants in the first and second of the joined cases – who were, at all times, represented by experienced counsel – that, unlike *Kennedy*, this was a case in which the general operation of these regimes required further elucidation, and in which the IPT, on account of its "extensive powers ... to investigate complaints before it and to access confidential information" would have been capable of providing a remedy.

9. There is, therefore, also no basis for any suggestion that our approach seeks, in any way, to overturn or "disapply" the Court's unanimous ruling in *Kennedy*. The simple fact is that, in our view, the two are clearly and obviously distinguishable.

10. Secondly, the first applicant, was clearly informed by the Government, in their response to the letter before action of 26 July 2013 (§ 19), that their complaints could be raised in the IPT, a court established specifically to hear allegations by citizens of wrongful interference with their communications as a result of conduct covered by that Act and a court endowed with exclusive jurisdiction to investigate any complaint that a person's communications have been intercepted and, where interception has occurred, to examine the authority for such interception. This letter was, of course, sent at around the same time as the ten human rights organisations which are the applicants in the third of the joined cases, no doubt recognising the need to have exhausted existing effective domestic remedies before applying to this Court, lodged their complaints before the IPT (June to December 2013; § 21). It was also four years after the UK Supreme Court, in its judgment in *R (on the application of A) v B* [2009] UKSC 12, had confirmed the exclusive jurisdiction of the IPT and its ability, as demonstrated by its decisions in *Kennedy* (IPT/01/62 & 77) and *The British-Irish Rights Watch and others v Security Service, GCHQ and the SIS* (IPT/01/77), to adjust the procedures before it as necessary so as to ensure that disputes before it can be determined justly.

11. Thirdly and in any event, even if, contrary to our view, the applicants in the first and second of the joined cases would have been entitled to rely on *Kennedy* at the time they lodged their applications with the Court they nevertheless accepted before this Court (§ 241), by reference to the judgment in *Campbell and Fell v. the United Kingdom*, 28 June 1984,

§§ 62-63, Series A no. 80, that in light of any finding by the Court to the effect that the IPT is an effective remedy, they would now be required to go back and exhaust unless it would be unjust to require them to do so. As these applicants' complaints concern the general operation of the impugned regimes, rather than specific complaints about an interference with their rights under the Convention, they would still be entitled to raise them before the IPT now.

12. Many of the complaints advanced in the first and second of the joined applications (including, in particular, all of those relating to the Chapter II regime, the sharing of non-intercept material with foreign governments and the lack of protection for confidential journalistic material and journalistic sources under the section 8(4) regime) were not addressed in the *Liberty* proceedings and have not yet been determined by the IPT. Consequently, there is no reason to doubt that if the applicants were now to raise those complaints before the IPT, they would have “a reasonable prospect of success”. In fact, in respect of the Chapter II complaint it may be thought that they would have a more than reasonable prospect of success. After all, as the majority records in § 463 of the judgment, the Government, in response to a challenge brought by Liberty, recently conceded that Part 4 of the IPA (which included a power to issue “retention notices” to telecommunications operators requiring the retention of data) was incompatible with fundamental rights in EU law: *R (The National Council for Civil Liberties (Liberty)) v Secretary of State for the Home Department & Anor* [2018] EWHC 975 (Admin). As Chapter II of RIPA, like Part 4 of the IPA, permits access to data for the purpose of combating crime (as opposed to “serious crime”), this concession led the majority to find a violation of Article 8 of the Convention in relation to the Chapter II regime (§ 467) which would suggest that the applicants had a strong basis for challenging, at the domestic level, the compliance of the Chapter II regime with EU law and, indeed, the Convention.

13. The same could not necessarily be said about those complaints raised by the first and/or second of the joined cases which were determined by the IPT in the *Liberty* proceedings; however, those issues were, of course, also raised by the applicants in the third of the joined cases and would therefore (and in fact have been) considered and determined by the Court on its merits.

14. As a result, and in clear contrast with the ultimate conclusion in *Campbell and Fell*, there is here therefore no evidence to suggest that “it would be unjust now to find these complaints inadmissible for failure to exhaust domestic remedies” (*ibid.* at § 63). Consequently, in our view, both the requirements of Article 35 § 5 of the Convention as well as the application of the principle of subsidiarity, in fact, required such a finding.

15. The point made in the judgment about the fundamental importance of the “elucidatory” role of the domestic courts is further underlined by the

BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT – 199
SEPARATE OPINIONS

complaint made in relation to the Chapter II regime. After all, as the judgment records in § 451, in both their application to the Court and their initial observations, the applicants in the second of the joined cases had incorrectly referred to the Chapter II regime as a regime for the interception of communications data; rather than a regime which permits certain public authorities to acquire communications data from Communications Service Providers (“CSPs”). This “fundamental legal misunderstanding” led the Government to submit *inter alia* that the applicants had put forward no factual basis whatsoever for concluding that their communications were acquired in this way, and that they did not contend that they had been affected, either directly or indirectly, by the regime.

16. As noted above, the Court’s conclusion on the Chapter II regime was, of course, ultimately based on the concession by the Government in *R (The National Council for Civil Liberties (Liberty)) v Secretary of State for the Home Department & Anor* [2018] EWHC 975 (Admin) which enabled the majority to find that the equivalent language in the Chapter II regime was “not in accordance with the law” within the meaning of Article 8 of the Convention (§ 467). However, had that not been the case, this Court would have been confronted with the task of considering in detail whether the regime’s attendant safeguards were sufficient to satisfy the requirements of the Convention; and that (1) on the basis of a case initially advanced on the basis of a “fundamental legal misunderstanding” about the nature of the regime, (2) without any assistance or findings by the IPT in relation to what the attendant safeguards, both above and below the waterline, in fact were and/or (3) any reasoned conclusion by the IPT as to whether or not they satisfied the requirements of Article 8 (or could be made to satisfy the requirements of Article 8 by means of further disclosure akin to that ordered on 9 October 2014 in the proceedings brought by the applicants in the third of the joined applications). This would plainly have been a wholly undesirable state of affairs.

The section 8(4) regime

17. As indicated above, there is much in the judgment of the majority we agree with.

18. Firstly, we agree with the majority (as well as with the unanimous judgment in *Centrum För Rättvisa*) in relation to the relevant general principles as set out in the judgment. In particular we agree with the affirmation by the majority (as well as the judgment in *Centrum För Rättvisa* and the report by the Venice Commission) that while the Court has considered prior judicial authorisation to be an important safeguard, and perhaps even “best practice”, it has also repeatedly confirmed that, by itself, such prior judicial authorisation is neither necessary nor sufficient to ensure compliance with Article 8 of the Convention (§ 320).

200 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT –
SEPARATE OPINIONS

19. Secondly, we also agree with the majority in identifying as potential shortcomings (or, to use the language in *Centrum För Rättvisa* “areas where there is scope for improvement”) in the operation of the section 8(4) regime “the lack of oversight of the entire selection process, including the selection of bearers for interception, the selectors and search criteria for filtering intercepted communications, and the selection of material for examination by an analyst; and secondly, the absence of any real safeguards applicable to the selection of related communications data for examination” (§ 387).

20. Finally, we agree with the majority as to the correct approach to be applied when considering whether the system under review satisfied the requirement of being “necessary in a democratic society” under Article 8 § 2 of the Convention, namely that:

“... regard must be had to the actual operation of the system of interception, including the checks and balances on the exercise of power, and the existence or absence of any evidence of actual abuse (see *Association for European Integration and Human Rights and Ekimdzhiiev*, cited above, § 92) (§ 320)

... it must principally have regard to the actual operation of a system of interception as a whole, including the checks and balances on the exercise of power, and the existence (or absence) of any evidence of actual abuse (...), such as the authorising of secret surveillance measures haphazardly, irregularly or without due and proper consideration (see *Roman Zakharov*, cited above, § 267) (§ 377).”

21. Where we disagree is (again) in the application of that approach to the system under review.

22. Before setting out in little more detail the basis for our disagreement we note in passing that this Court’s underlying approach appears to be in clear contrast to the approach taken by the CJEU in *Digital Rights Ireland v. Minister for Communications, Marine and Natural Resources and Others and Settinger and Others* (Cases C-293/12 and C-594/12) and *Secretary of State for the Home Department v. Watson and Others* (C-698/15). In the former case, the CJEU was considering the validity of the Data Retention Directive, and in the latter, the validity of domestic legislation containing the same provisions as that directive. While its focus was on the retention of data by CSPs, it also considered the question of access to retained data by the national authorities. In doing so, it indicated that access should be limited to what was strictly necessary for the objective pursued and, where that objective was fighting crime, it should be restricted to fighting serious crime. It further suggested that access should be subject to prior review by a court or independent administrative authority, and that there should be a requirement that the data concerned be retained within the European Union. Therefore, while there is some similarity in the language used by the two courts, the CJEU appears to have adopted a more prescriptive approach as regards the safeguards it considers necessary. This may be due to the fact that in both cases it was considering the rights guaranteed by reference to Articles 7 (Respect for private and family life) and 8 (Protection of personal

BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT – 201
SEPARATE OPINIONS

data) of the Charter of Fundamental Rights. However, while in *Watson* the CJEU declined to state whether the protection provided by Articles 7 and 8 of the Charter was wider than that afforded by Article 8 of the Convention, we can but note that, on the one hand, Article 52 § 3 of the Charter of Fundamental Rights, while recognising the ability of EU law providing more extensive protection, is clearly expressed by reference to “rights” guaranteed by the Convention (rather than “Articles”) corresponding to “rights” contained in the Charter and that, on the other hand, this Court has, at least since the 1978 judgment of the Plenary Court in *Klass and Others v. Germany*, Series A no. 28, consistently protected the right to the protection of personal data under Article 8 of the Convention. In any event, in *Ben Faiza v. France*, no. 31446/12, 8 February 2018, which was decided one year after *Watson*, and four years after *Digital Rights Ireland*, this Court did not follow the CJEU’s approach, preferring instead to follow its well-established approach and to review the impugned regime as a whole in order to evaluate the adequacy of the available safeguards.

23. In any event, applying this Court’s well-established approach, it is in our view, clear from the (in the context of secret surveillance cases unusually) extensive and detailed (publicly available) evidence in relation to the operation of the section 8(4) regime (summarised over some 35 pages in the judgment) that, despite the identified areas where there is scope for improvement, these are not, in themselves, sufficiently significant to justify the conclusion that “the section 8(4) regime does not meet the ‘quality of law’ requirement and is incapable of keeping the ‘interference’ to what is ‘necessary in a democratic society’” (§ 388). On the contrary, adopting the approach of this Court in *Centrum För Rättvisa*, § 181, it is clear in our view that, making an overall assessment and having regard to the margin of appreciation enjoyed by the national authorities in protecting national security, the section 8(4) regime does provide adequate and sufficient guarantees against arbitrariness and the risk of abuse. As a result, we concluded that the relevant legislation meets the “quality of law” requirement and the “interference” established can be considered as being “necessary in a democratic society” and that there was, therefore, no violation of Article 8 of the Convention.

24. In this context, the contrast to the judgment in *Centrum För Rättvisa* is instructive. After all, in that case the Court applied the same general principles to the Swedish bulk interception regime and concluded, unanimously, that there was no breach of Article 8 of the Convention. Conscious of the difficulty – at times – in making detailed meaningful comparisons between different interception regimes, it is nevertheless noteworthy that the regime under consideration in that case, while equipped with judicial prior authorisation:

(a) was completely shrouded in secrecy with the Court having little meaningful information at all either about the actual generic operation of

202 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT –
SEPARATE OPINIONS

the system (including the actual operation of the Foreign Intelligence Court (“FIC”) itself) or the impact of the system on and/or operation of safeguards in relation to any individual;

(b) provided that, in principle, the FIC should hold public hearings but found that there has never been a public hearing, all decisions are confidential and no information is disclosed to the public about the number of hearings, the number of permits granted or rejected, the reasoning of the court’s decisions or the amount or type of search terms being used. While the FIC is assisted by the “privacy protection representative” whose role it is to protect the “interests of the general public” he or she does not appear on behalf of or represent the interests of any affected individual. Furthermore, the privacy protection representative cannot appeal against a decision by the FIC or “report any perceived irregularities to the supervisory bodies”;

(c) was concerned with interception by the National Defence Radio Establishment (“FRA”) on behalf of, and which, therefore, required communication of the intercept material to, a much wider group “clients” (“the Government, the Government Offices, the Armed Forces and, as from January 2013, the Security Police and the National Operative Department of the Police Authority”);

(d) provided for authorisation of interception for a greater number (eight) of “purposes” (“1) external military threats to the country, 2) conditions for Swedish participation in international peacekeeping or humanitarian missions or threats to the safety of Swedish interests in the performance of such operations, 3) strategic circumstances concerning international terrorism or other serious cross-border crimes that may threaten essential national interests, 4) the development and proliferation of weapons of mass destruction, military equipment and other similar specified products, 5) serious external threats to society’s infrastructure, 6) foreign conflicts with consequences for international security, 7) foreign intelligence operations against Swedish interests, and 8) the actions or intentions of a foreign power that are of substantial importance for Swedish foreign, security or defence policy”);

(e) had similar difficulties to those identified in relation to the UK regime to separate out non-external communications between a sender and receiver within the respective State at the point of collection;

(f) allows for the communication of intercept product not only to other states but also to “international organisations” (not further defined) where that is “not prevented by secrecy and if necessary for the FRA to perform its activities within international defence and security cooperation” and “it is beneficial for the Swedish government or Sweden’s comprehensive defence strategy” and without any provision requiring the third country/international organisation recipient to protect

BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT – 203
SEPARATE OPINIONS

the data with the same or similar safeguards as those applicable internally; and

(g) provided for an obligation to notify the subject of an intercept after the event; an obligation which, however, “had never been used by the FRA, due to secrecy.

25. Considering the accepted difficulty in making a meaningful comparison between two or more distinct interception regime together with the different conclusions reached by this Court at about the same time, in our view, further underlines the importance of the Court adopting an approach of asking whether, taking “an overall assessment and having regard to the margin of appreciation enjoyed by the national authorities in protecting national security” the system adopted provides adequate and sufficient guarantees against arbitrariness and the risk of abuse, even if there may be individual aspects of any system which might be capable of being altered or improved. Such an approach properly reflects the role of the Convention, which is to set down “minimum standards” that can be applied across all Member States. Provided that – following an overall assessment – the Court finds that a system for bulk interception provides adequate and sufficient guarantees against arbitrariness and abuse, in view of the very different regimes in operation in different States, it will not be appropriate for it to be too prescriptive about the way in which those regimes should operate (although it may, as it did both in *Centrum För Rättvisa* and in this case, identify those aspects of the regime which could be improved upon). Applying this approach to the Court’s supervisory jurisdiction in the present case (as it was in *Centrum För Rättvisa*), the Court should have given due weight to the fact that the domestic courts and authorities have subjected both the UK system as a whole as well as the individual complaints at issue to detailed and extensive scrutiny by express reference to the Convention standards and this Court’s case law and should have found that there was, here, no breach of Article 8 of the Convention.

Post Scriptum

26. Since the adoption of this judgment on 3 July 2018, the IPT has handed down yet another judgment in relation to another, unrelated, aspect of the UK’s surveillance regime: *Privacy International v Secretary of State for Foreign and Commonwealth Affairs (Rev 1)* [2018] UKIPTrib IPT_15_110_CH (23 July 2018). For obvious reasons this judgment was not available for consideration by the Court when it reached its conclusions on the question of exhaustion of domestic remedies (and we have heard no submissions on it). That said, it seems to us that this careful and detailed judgment provides yet further support (if any was necessary) that, in principle, the IPT is an effective remedy for the purposes of Article 35 § 1

204 BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM JUDGMENT –
SEPARATE OPINIONS

of the Convention which applicants will be required to have exhausted
before this Court has jurisdiction to entertain their application.

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 24



NSA Director of Civil Liberties and Privacy Office Report

NSA's Implementation of Foreign Intelligence Surveillance Act Section 702

April 16, 2014



National Security Agency, Civil Liberties and Privacy Office
Report
NSA's Implementation of Foreign Intelligence Surveillance Act Section 702

April 16, 2014

INTRODUCTION

This report was prepared by the National Security Agency (NSA) Civil Liberties and Privacy Office as part of its responsibilities to enhance communications and transparency with the public and stakeholders. Its Director is the primary advisor to the Director of NSA when it comes to matters of civil liberties and privacy. Created in January 2014, the Office is also charged with ensuring that civil liberties and privacy protection are integrated into NSA activities. The intent of this paper is to help build a common understanding that can serve as a foundation for future discussions about the existing civil liberties and privacy protections.

The mission of NSA is to make the nation safer by providing policy makers and military commanders with timely foreign intelligence and by protecting national security information networks. NSA collects foreign intelligence based on requirements from the President, his national security team, and their staffs through the National Intelligence Priorities Framework. NSA fulfills these national foreign intelligence requirements through the collection, processing, and analysis of communications or other data, passed or accessible by radio, wire or other electronic means.

NSA's authority to conduct signals intelligence collection for foreign intelligence and counterintelligence purposes is provided primarily by Section 1.7(c)(1) of Executive Order 12333, as amended. The execution of NSA's signals intelligence mission must be conducted in conformity with the Fourth Amendment. This includes NSA's acquisition of communications to which a U.S. person is a party under circumstances in which the U.S. person has a reasonable expectation of privacy. The Foreign Intelligence Surveillance Act of 1978 (FISA) further regulates certain types of foreign intelligence collection, including that which occurs with compelled assistance from U.S. communications providers.

This Report describes one way in which NSA meets these responsibilities while using Section 702 of FISA, as amended by the FISA Amendments Act of 2008. Although multiple federal agencies participate in Section 702 collection, this paper describes the process by which NSA obtains, uses, shares, and retains communications of foreign intelligence value pursuant to Section 702. It also describes existing privacy and civil liberties protections built into the process.



The NSA Civil Liberties and Privacy Office (CLPO) used the Fair Information Practice Principles (FIPP)¹ as an initial tool to describe the existing civil liberties and privacy protections in place for collection done under Section 702 authority.²

SECTION 702 OF FISA

Section 702 of FISA was widely and publicly debated in Congress both during the initial passage in 2008 and the subsequent re-authorization in 2012. It provides a statutory basis for NSA, with the compelled assistance of electronic communication service providers, to target non-U.S. persons reasonably believed to be located outside the U.S. in order to acquire foreign intelligence information. Given that Section 702 only allows for the targeting of non-U.S. persons outside the U.S., it differs from most other sections of FISA. It does not require an individual determination by the U.S. Foreign Intelligence Surveillance Court (FISC) that there is probable cause to believe the target is a foreign power or an agent of a foreign power. Instead, the FISC reviews annual topical certifications executed by the Attorney General (AG) and the Director of National Intelligence (DNI) to determine if these certifications meet the statutory requirements. The FISC also determines whether the statutorily required targeting and minimization procedures used in connection with the certifications are consistent with the statute and the Fourth Amendment. The targeting procedures are designed to ensure that Section 702 is only used to target non-U.S. persons reasonably believed to be located outside the U.S.

The minimization procedures are designed to minimize the impact on the privacy on U.S. persons by minimizing the acquisition, retention, and dissemination of non-publicly available U.S. person information that was lawfully, but incidentally acquired under Section 702 by the targeting of non-U.S. persons reasonably believed to be located outside the U.S. Under these certifications the AG and the DNI issue directives to electronic communication service providers (service providers) that require these service providers to “immediately provide the Government with all information ... or assistance necessary to accomplish the acquisition [of foreign intelligence information] in a manner that will protect the secrecy of the acquisition...” The Government’s acquisition of communications under its Section 702 authority thus takes place pursuant to judicial review and with the knowledge of the service providers.

NSA cannot intentionally use Section 702 authority to target any U.S. citizen, any other U.S. person, or anyone known at the time of acquisition to be located within the U.S. The statute also prohibits the use of Section 702 to intentionally acquire any communication as to which the

¹ The FIPPS are the recognized principles for assessing privacy impacts. They have been incorporated into EO13636, *Improving Critical Infrastructure Cybersecurity* and the National Strategy for Trusted Identities in Cyberspace. These principles are rooted in the U.S. Department of Health, Education and Welfare’s seminal 1973 report, “Records, Computers and the Rights of Citizens.” The FIPPs have been implemented in the Privacy Act of 1974, with certain exemptions, including ones that apply to certain national security and law enforcement activities.

² NSA CLPO will continue to refine its assessment tools to best suit the mission of NSA, as a member of the Intelligence Community, and to protect civil liberties and privacy.



sender and all intended recipients are known at the time of acquisition to be located inside the U.S. Similarly, the statute prohibits the use of Section 702 to conduct “reverse targeting” (i.e., NSA may not intentionally target a person reasonably believed to be located outside of the U.S. if the purpose of such acquisition is to target a person reasonably believed to be located inside the U.S.). All acquisitions conducted pursuant to Section 702 must be conducted in a manner consistent with the Fourth Amendment. NSA’s FISC-approved targeting procedures permit NSA to target a non-U.S. person reasonably believed to be located outside the U.S. if the intended target possesses, is expected to receive, and/or is likely to communicate foreign intelligence information concerning one of the certifications executed by the AG and DNI. Although the purpose of Section 702 is to authorize targeting of non-U.S. persons outside the U.S., the statute’s requirement for minimization procedures recognizes that such targeted individuals or entities may communicate about U.S. persons or with U.S. persons. For this reason, NSA also must follow FISC-approved minimization procedures that govern the handling of any such communications.

NSA must report to the Office of the Director of National Intelligence (ODNI) and the Department of Justice (DOJ) any and all instances where it has failed to comply with the targeting and/or minimization procedures. In addition, ODNI and DOJ have access to documentation concerning each of NSA’s Section 702 targeting decisions and conduct regular reviews in order to provide independent oversight of NSA’s use of the authority. The FISC Rules of Procedure require the Government to notify the Court of all incidents of non-compliance with applicable law or with an authorization granted by the Court. The Government reports Section 702 compliance incidents to the Court via individual notices and quarterly reports. In addition, the Government reports all Section 702 compliance incidents to Congress in the Attorney General’s Semiannual Report. Depending on the type or severity of compliance incident, NSA may also promptly notify the Congressional Intelligence Committees, as well as the President’s Intelligence Oversight Board of an individual compliance matter.

Existing Privacy and Civil Liberties Protections: Each of the three branches of federal government oversees NSA’s use of the Section 702 authorities. NSA provides transparency to its oversight bodies (Congress, DOJ, ODNI, DoD, the President’s Intelligence Oversight Board and the FISC) through regular briefings, court filings, and incident reporting. In addition, DOJ and ODNI conduct periodic reviews of NSA’s use of the authority and report on those reviews. More recently, at the direction of the President, the Government has provided additional transparency to the public regarding the program by declassifying FISC opinions and related documents. Although FISA surveillance is normally kept secret from the targets of the surveillance, there are exceptions. For example, if the Government intends to use the results of FISA surveillance, to include Section 702 surveillance, in a trial or other proceeding against a person whose communications were collected, the Government must notify the person so the person can challenge whether the communications were acquired lawfully. These protections implement the general Fair Information Practice Principle (FIPP) of transparency.



HOW NSA IMPLEMENTS SECTION 702 of FISA

TRAINING

Before an analyst gains access to any NSA signals intelligence data, the analyst must complete specialized training on the legal and policy guidelines that govern the handling and use of the data. Additional training is required for access to Section 702 data. These annual mandatory training requirements include scenario-based training, required reading, and a final competency test. The analyst must pass this test before being granted access. Furthermore, if a compliance incident involves a mistake or misunderstanding of relevant policies, the analyst is re-trained in order to continue to have access to the data acquired pursuant to Section 702.

IDENTIFYING AND TASKING A SELECTOR

Next in the Section 702 process is for an NSA analyst to identify a non-U.S. person located outside the U.S. who has and/or is likely to communicate foreign intelligence information as designated in a certification. For example, such a person might be an individual who belongs to a foreign terrorist organization or facilitates the activities of that organization's members. Non-U.S. persons are not targeted unless NSA has reason to believe that they have and/or are likely to communicate foreign intelligence information as designated in a certification; U.S. persons are never targeted.

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).

Next the NSA analyst must verify that there is a connection between the target and the selector and that the target is reasonably believed to be (a) a non-U.S. person and (b) located outside the U.S. This is not a 51% to 49% “foreignness” test. Rather the NSA analyst will check multiple sources and make a decision based on the totality of the information available. If the analyst discovers any information indicating the targeted person may be located in the U.S. or that the target may be a U.S. person, such information must be considered. In other words, if there is conflicting information about the location of the person or the status of the person as a non-U.S. person, that conflict must be resolved before targeting can occur.

For each selector, the NSA analyst must document the following information: (1) the foreign intelligence information expected to be acquired, as authorized by a certification, (2) the information that would lead a reasonable person to conclude the selector is associated with a



non-U.S. person, and (3) the information that would similarly lead a reasonable person to conclude that this non-U.S. person is located outside the U.S. This documentation must be reviewed and approved or denied by two senior NSA analysts who have satisfied additional training requirements. The senior NSA analysts may ask for more documentation or clarification, but regardless must verify that all requirements have been met in full. NSA tracks the submission, review, and approval process through the documentation and the senior NSA analysts' determinations are retained for further review by NSA's compliance elements, as well as external oversight reviewers from DOJ and ODNI. Upon approval, the selector may be used as the basis for compelling a service provider to forward communications associated with the given selector. This is generally referred to as "tasking" the selector.

Existing Privacy and Civil Liberties Protections: NSA trains its analysts extensively through a variety of means to ensure that analysts fully understand their responsibilities and the specific scope of this authority. If the analyst fails to meet the training standards, the analyst will not have the ability to use the Section 702 authority for collection purposes. If the analyst fails to maintain ongoing training standards, the analyst will lose the ability to use the Section 702 authority for collection purposes and all ability to retrieve any data previously collected under the authority. NSA requires any authorized and trained analyst seeking to task a selector using Section 702 to document the three requirements for use of the authority – that the target is connected sufficiently to the selector for an approved foreign intelligence purpose, that the target is a non-U.S. person, and that the target is reasonably believed to be located outside the U.S. This documentation must be reviewed, validated, and approved by the senior analysts who have received additional training. These protections implement the general FIPPs of purpose specification, accountability and auditing, and minimization.

ACCESSING AND ASSESSING COMMUNICATIONS OBTAINED UNDER SECTION 702 AUTHORITY

Once senior analysts have approved a selector as compliant, the service providers are legally compelled to assist the government by providing the relevant communications. Therefore, tasking under this authority takes place with the knowledge of the service providers. NSA receives information concerning a tasked selector through two different methods.

In the first, the Government provides selectors to service providers through the FBI. The service providers are compelled to provide NSA with communications to or from these selectors. This has been generally referred to as the PRISM program.

In the second, service providers are compelled to assist NSA in the lawful interception of electronic communications to, from, or about tasked selectors. This type of compelled service provider assistance has generally been referred to as Upstream collection. NSA's FISC-approved targeting procedures include additional requirements for such collection designed to prevent acquisitions of wholly domestic communications. For example, in certain circumstances NSA's procedures require that it employ an Internet Protocol filter to ensure that the target is



located overseas. The process for approving the selectors for tasking is the same for both PRISM and Upstream collection.

Once NSA has received communications of the tasked selector, NSA must follow additional FISC-approved procedures known as the minimization procedures. These procedures require NSA analysts to review at least a sample of communications acquired from all selectors tasked under Section 702, which occurs on a regular basis to verify that the reasonable belief determination used for tasking remains valid.

The NSA analyst must review a sample of communications received from the selectors to ensure that they are in fact associated with the foreign intelligence target and that the targeted individual or entity is not a U.S. person and is not currently located in the U.S. If the NSA analyst discovers that NSA is receiving communications that are not in fact associated with the intended target or that the user of a tasked selector is determined to be a U.S. person or is located in the U.S., the selector must be promptly “detasked.” As a general rule, in the event that the target is a U.S. person or in the U.S., all other selectors associated with the target also must be detasked.

Existing Privacy and Civil Liberties Protections: In addition to extensive training, the analyst is required to review the collection to determine that it is associated with the targeted selector and is providing the expected foreign intelligence shortly after the tasking starts and at least annually thereafter. This review allows NSA to identify possible problems with the collection and provides an additional layer of accountability. In addition, NSA has technical measures that alert the NSA analysts if it appears a selector is being used from the U.S. These protections implement the general FIPPs of purpose specification, minimization, accountability and auditing, data quality, and security.

NSA PROCESSING AND ANALYSIS OF COMMUNICATIONS OBTAINED UNDER SECTION 702 AUTHORITY

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, such as the time and duration of a telephone call, or sending and receiving email addresses.

NSA analysts may access communications obtained under Section 702 authority for the purpose of identifying and reporting foreign intelligence. They access the information via “queries,” which may be date-bound, and may include alphanumeric strings such as telephone numbers, email addresses, or terms that can be used individually or in combination with one another. FISC-approved minimization procedures govern any queries done on Section 702-derived information. NSA analysts with access to Section 702-derived information are trained in the proper construction of a query so that the query is reasonably likely to return valid foreign



intelligence and minimizes the likelihood of returning non-pertinent U.S. person information. Access by NSA analysts to each repository is controlled, monitored, and audited. There are, for example, automated checks to determine if an analyst has completed all required training prior to returning information responsive to a query. Further, periodic spot checks on queries by NSA analysts are conducted.

Since October 2011 and consistent with other agencies' Section 702 minimization procedures, NSA's Section 702 minimization procedures have permitted NSA personnel to use U.S. person identifiers to query Section 702 collection when such a query is reasonably likely to return foreign intelligence information. NSA distinguishes between queries of communications content and communications metadata. NSA analysts must provide justification and receive additional approval before a content query using a U.S. person identifier can occur. To date, NSA analysts have queried Section 702 content with U.S. person identifiers less frequently than Section 702 metadata. For example, NSA may seek to query a U.S. person identifier when there is an imminent threat to life, such as a hostage situation. NSA is required to maintain records of U.S. person queries and the records are available for review by both DOJ and ODNI as part of the external oversight process for this authority. Additionally, NSA's procedures prohibit NSA from querying Upstream data with U.S. person identifiers.

Existing Privacy and Civil Liberties Protections: In addition to the training and access controls, NSA maintains audit trails for all queries of the Section 702 data. NSA's Signals Intelligence Directorate's compliance staff routinely reviews a portion of all queries that include U.S. person identifiers to ensure that all such queries are only conducted when appropriate. Personnel from DOJ and ODNI provide an additional layer of oversight to ensure that NSA is querying the data appropriately. These protections implement the general FIPPs of security, accountability and auditing, and data quality.

NSA DISSEMINATION OF INTELLIGENCE DERIVED FROM COMMUNICATIONS OBTAINED UNDER SECTION 702 AUTHORITY

NSA only generates signals intelligence reports when the information meets a specific intelligence requirement, regardless of whether the proposed report contains U.S. person information. Dissemination of information about U.S. persons in any NSA foreign intelligence report is expressly prohibited unless that information is necessary to understand foreign intelligence information or assess its importance, contains evidence of a crime, or indicates a threat of death or serious bodily injury. Even if one or more of these conditions apply, NSA may include no more than the minimum amount of U.S. person information necessary to understand the foreign intelligence or to describe the crime or threat. For example, NSA typically "masks" the true identities of U.S. persons through use of such phrases as "a U.S. person" and the suppression of details that could lead to him or her being successfully identified by the context. Recipients of NSA reporting can request that NSA provide the true identity of a masked U.S. person referenced in an intelligence report if the recipient has a legitimate need to know the identity. Under NSA policy, NSA is allowed to unmask the identity only under certain



conditions and where specific additional controls are in place to preclude its further dissemination, and additional approval has been provided by one of seven designated positions at NSA. Additionally, together DOJ and ODNI review the vast majority of disseminations of information about U.S. persons obtained pursuant to Section 702 as part of their oversight process.

Existing Privacy and Civil Liberties Protections: As noted above, NSA only generates signals intelligence reports when the information meets a specific intelligence requirement, regardless of whether the proposed report contains U.S. person information or not. Additionally, NSA's Section 702 minimization procedures require any U.S. person information to be minimized prior to dissemination, thereby reducing the impact on privacy for U.S. persons. The information may only be unmasked in specific instances consistent with the minimization procedures and NSA policy. These protections implement the general FIPPs of minimization and purpose specification.

RETENTION OF UNEVALUATED COMMUNICATIONS OBTAINED UNDER SECTION 702 AUTHORITY

The maximum time that specific communications' content or metadata may be retained by NSA is established in the FISC-approved minimization procedures. The unevaluated content and metadata for PRISM or telephony data collected under Section 702 is retained for no more than five years. Upstream data collected from Internet activity is retained for no more than two years. NSA complies with these retention limits through an automated process.

NSA's procedures also specify several instances in which NSA must destroy U.S. person collection promptly upon recognition. In general, these include any instance where NSA analysts recognize that such collection is clearly not relevant to the authorized purpose of the acquisition nor includes evidence of a crime. Additionally, absent limited exceptions, NSA must destroy any communications acquired when any user of a tasked account is found to have been located in the U.S. at the time of acquisition.

Existing Privacy and Civil Liberties Protections: NSA has policies, technical controls, and staff in place to ensure the data is retained in accordance with the FISC-approved procedures. The automated process to delete the collection at the end of the retention period applies to both U.S. person and non U.S. person the information. There is an additional manual process for the destroying information related to U.S. Persons where NSA analysts have recognized the collection is clearly not relevant to the authorized purpose of the acquisition nor includes evidence of a crime. These protections implement the general FIPPs of minimization and security.



ORGANIZATIONAL MANAGEMENT, COMPLIANCE, AND OVERSIGHT

NSA is subject to rigorous internal compliance and external oversight. Like many other regulated entities, NSA has an enterprise-wide compliance program, led by NSA's Director of Compliance, a position required by statute. NSA's compliance program is designed to provide precision in NSA's activities to ensure that they are consistently conducted in accordance with law and procedure, including in this case the Section 702 certifications and accompanying Section 702 targeting and minimization procedures and additional FISC requirements. As part of the enterprise-wide compliance structure, NSA has compliance elements throughout its various organizations. NSA also seeks to detect incidents of non-compliance at the earliest point possible. When issues of non-compliance arise regarding the way in which NSA carries out the FISC-approved collection, NSA takes corrective action and, in parallel, NSA must report incidents of non-compliance to ODNI and DOJ for further reporting to the FISC and Congress, as appropriate or required.

These organizations, along with the NSA General Counsel, the NSA Inspector General, and most recently the Director of Civil Liberties and Privacy have critical roles in ensuring all NSA operations proceed in accordance with the laws, policies, and procedures governing intelligence activities. Additionally, each individual NSA analyst has a responsibility for ensuring that his or her personal activities are similarly compliant. Specifically, this responsibility includes recognizing and reporting all situations in which he or she may have exceeded his or her authority to obtain, analyze, or report intelligence information under Section 702 authority.

Compliance: NSA reports all incidents in which, for example, it has or may have inappropriately queried the Section 702 data, or in which an analyst may have made typographical errors or dissemination errors. NSA personnel are obligated to report when they believe NSA is not, or may not be, acting consistently with law, policy, or procedure. If NSA is not acting in accordance with law, policy, or procedure, NSA will report through its internal and external intelligence oversight channels, conduct reviews to understand the root cause, and make appropriate adjustments to its procedures.

If NSA discovers that it has tasked a selector that is used by a person in the U.S. or by a U.S. person, then NSA must cease collection immediately and, in most cases must also delete the relevant collected data and cancel or revise any disseminated reporting based on this data. NSA encourages self-reporting by its personnel and seeks to remedy any errors with additional training or other measures as necessary. Following an incident, a range of remedies may occur: admonishment, written explanation of the offense, request to acknowledge a training point that the analyst might have missed during training, and/or required retesting. In addition to reporting described above, any intentional violation of law would be referred to the NSA Office of Inspector General. To date there have been no such instances, as most recently confirmed by the President's Review Group on Intelligence and Communications Technology.



External Oversight: As required by the Section 702 targeting procedures, both DOJ and ODNI conduct routine oversight reviews. Representatives from both agencies visit NSA on a bi-monthly basis. They examine all tasking datasheets that NSA provides to DOJ and ODNI to determine whether the tasking sheets meet the documentation standards required by NSA's targeting procedures and provide sufficient information for the reviewers to ascertain the basis for NSA's foreignness determinations. For those records that satisfy the standards, no additional documentation is requested. For those records that warrant further review, NSA provides additional information to DOJ and ODNI during or following the onsite review. NSA receives feedback from the DOJ and ODNI team and incorporates this information into formal and informal training to analysts. DOJ and ODNI also review the vast majority of disseminated reporting that includes U.S. person information.

Existing Privacy and Civil Liberties Protections: The compliance and oversight processes allow NSA to identify any concerns or problems early in the process so as to minimize the impact on privacy and civil liberties. These protections implement the general FIPPs of transparency to oversight organizations and accountability and auditing.

CONCLUSION

This Report, prepared by NSA's Office of Civil Liberties and Privacy, provides a comprehensive description of NSA's Section 702 activities. The report also documents current privacy and civil liberties protections.

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 25

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

An intrusion-detection system known as EINSTEIN 2.0 used to protect civilian unclassified networks in the Executive Branch against malicious network activity complies with the Fourth Amendment to the Constitution, the Wiretap Act, the Foreign Intelligence Surveillance Act, the Stored Communications Act, and the pen register and trap and trace provisions of chapter 206 of title 18, United States Code, provided that certain log-on banners or computer-user agreements are consistently adopted, implemented, and enforced by executive departments and agencies using the system.

January 9, 2009

MEMORANDUM OPINION FOR THE COUNSEL TO THE PRESIDENT

As part of the Comprehensive National Cybersecurity Initiative, the Department of Homeland Security (“DHS”), in coordination with the Office of Management and Budget, is in the process of establishing an intrusion-detection system known as EINSTEIN 2.0 in order to detect unauthorized network intrusions and data exploitations against the Executive Branch’s civilian unclassified computer systems (“Federal Systems”).¹ In January 2007, you asked this Office to undertake a legal review of proposed EINSTEIN 2.0 operations; since that time we have provided ongoing informal advice regarding the legality of those operations, which are now underway. This memorandum formalizes the informal advice we have provided regarding whether EINSTEIN 2.0 operations comply with the Fourth Amendment to the Constitution of the United States, title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 211, 18 U.S.C. § 2510 *et seq.* (2006), as amended (“the Wiretap Act”), the Foreign Intelligence Surveillance Act, Pub. L. No. 95-511, 92 Stat. 1783, 50 U.S.C.A. § 1801 *et seq.* (West 2008), as amended (“FISA”), the Stored Communications Act, Pub. L. No. 99-508, Tit. II, 100 Stat. 1848 (1986), 18 U.S.C. § 2701 *et seq.* (2006), as amended (“SCA”), and the pen register and trap and trace provisions of title 18, United States Code, 18 U.S.C. § 3121 *et seq.* (2006), as amended (“Pen/Trap Act”).

We examine these legal issues in the context of an executive department’s or agency’s use of a model computer log-on banner or a model computer-user agreement developed by lawyers from the Department of Justice (“DOJ”), DHS, and other departments and agencies with expertise in cybersecurity issues. We conclude that as long as executive departments and agencies participating in EINSTEIN 2.0 operations consistently adopt, implement, and enforce the model log-on banner or computer-user agreement—or log-on banners or computer-user agreements with terms that are substantially equivalent to those models—the use of EINSTEIN 2.0 technology to detect computer network intrusions and exploitations against Federal Systems complies with the Fourth Amendment, the Wiretap Act, FISA, the SCA, and the Pen/Trap Act.

¹ As used this memorandum, the term “Federal Systems” includes all Executive Branch federal Government information systems except for National Security Systems of executive departments and agencies and Department of Defense information systems.

*Opinions of the Office of Legal Counsel in Volume 33***I.**

Over the past several years, Federal Systems have been subject to sophisticated and well-coordinated computer network intrusions and exploitations on an unprecedented scale. The Intelligence Community has determined that those malicious network activities pose a grave threat to national security. *See also* Center for Strategic and International Studies, *Securing Cyberspace* 11-15 (2008) (discussing national security implications of federal network vulnerabilities). Those malicious network activities occur at the hands of hostile foreign nations (including foreign intelligence services), transnational criminal groups and enterprises, and individual computer hackers. Recent intrusions and exploitations have resulted in the theft of significant amounts of unclassified data from many executive departments and agencies, as well as information regarding the vulnerabilities of Federal Systems. The unclassified networks of the Departments of Defense, State, Homeland Security, and Commerce, among others, have suffered intrusions against their networks and exploitations of their data. Accordingly, the Homeland Security Council has determined that the deployment of a multi-layered network defense system is necessary to protect Federal Systems against these ongoing computer intrusions and exploitations carried out by a broad array of cyber adversaries.

The first layer of this network-defense system is known as EINSTEIN 1.0 and already is in place across segments of several Executive Branch agencies. EINSTEIN 1.0 is a semi-automated process for detecting—albeit after the fact—inappropriate or unauthorized inbound and outbound network traffic between participating departments and agencies and the Internet. The United States Computer Emergency Readiness Team (“US-CERT”), an organizational component of DHS, administers EINSTEIN 1.0.

EINSTEIN 1.0 analyzes only “packet header” information—and not packet “payload” (content) information—for inbound and outbound Internet traffic of participating agencies.² The header information collected by EINSTEIN 1.0 technology includes: the source and destination IP addresses for the packet, the size of the data packet, the specific Internet protocol used (for e-mail, the Simple Mail Transfer Protocol and, for use of the World Wide Web, the Hypertext Transport Protocol), and the date and time of transmission of the packet (known as “the date/time stamp”). EINSTEIN 1.0 collects this information only after packets already have been sent or received by a user, and, thus, does not provide real-time information regarding network intrusions and exploitations against Federal Systems. US-CERT analysts examine the header information to identify suspicious inbound and outbound Internet traffic, particularly network backdoors and intrusions, network scanning activities, and computer network exploitations using viruses, worms, spyware, bots, Trojan horses, and other “malware.”

² The Internet consists of millions of computers connected by a network of fiber-optic cables and other data-transmission facilities. Data transmitted across the Internet are broken down into “packets” that are sent out from one computer to another. Each packet is directed (routed) to its intended source from its respective destination by an Internet Protocol (“IP”) address. An IP address is a unique numerical address, akin to a phone number or physical address, identifying each computer on the Internet. Each packet may follow a different route to its ultimate IP address destination, traveling over the networks of several different Internet backbone providers and Internet Service Providers (“ISPs”) before arriving at the destination. Upon arrival at the destination, the packets are reconstituted. *See generally* Jonathan E. Nuechterlein & Philip J. Weiser, *Digital Crossroads* 121-28 (2005).

EINSTEIN 1.0 contains several limitations. First, it does not provide real-time reporting regarding intrusions and exploitations against Federal Systems. Second, it does not cover all Federal Systems, and, therefore, does not provide complete awareness regarding malicious network activity directed against those systems. Third, because EINSTEIN 1.0 does not scan packet content, it does not offer complete intrusion and exploitation detection functionality.

We understand that many executive departments and agencies supplement EINSTEIN 1.0 with their own intrusion-detection systems, which are designed to identify network intrusions and exploitations conducted against their own computer systems. In addition, individual departments and agencies also operate their own network filters to block certain unauthorized content, such as Internet pornography and file-sharing activities, among others. We understand, however, that there is little or no coordination or communication among Executive Branch entities conducting these individualized network defense activities. Accordingly, multiple departments facing the same intrusion or exploitation might have no idea that they are all facing a coordinated malicious network operation. Nor would departments or agencies that have not yet been subject to the intrusion or exploitation have advanced warning of the activity, such that they could upgrade their defenses. Hence, the lack of cybersecurity collaboration within the Executive Branch leads to inefficient network defensive measures that contribute to the ongoing vulnerability of Federal Systems.

To rectify this situation, DHS, in conjunction with OMB, is deploying throughout the Executive Branch an intrusion-detection system known as EINSTEIN 2.0 to provide greater coordination and situational awareness regarding malicious network activities directed against Federal Systems. EINSTEIN 2.0 is a robust system that is expected to overcome the technical limitations of EINSTEIN 1.0. EINSTEIN 2.0 technology is comprised of computers (“sensors”) configured with commercial “off-the-shelf” intrusion-detection software as well as government-developed software. That technology will be located at certain Internet access points known as Trusted Internet Connections (“TICs”), which connect Federal Systems to the Internet.

EINSTEIN 2.0 intrusion-detection sensors will observe in near-real time the packet header and packet content of all incoming and outgoing Internet traffic of Federal Systems (“Federal Systems Internet Traffic”) for the “signatures” of malicious computer code used to gain access to or to exploit Federal Systems.³ *See generally* NIST Special Publication No. 800-94 (2007) (discussing signature-based detection techniques). Because Internet traffic is IP-address based, we understand that only Federal Systems Internet Traffic destined to or sent from an IP address associated with an executive department or agency participating in EINSTEIN 2.0 (“EINSTEIN 2.0 Participant”) would be scanned by EINSTEIN 2.0 technology. Thus, EINSTEIN 2.0 technology will scan only the Federal Systems Internet Traffic for EINSTEIN 2.0 Participants that connect to the Internet at TICs.

DHS has the responsibility for determining which signatures to program into the EINSTEIN 2.0 sensors, pursuant to procedures developed by DHS. Signatures may be derived

³ By the term “malicious computer code,” we mean not only “malware,” such as viruses, spyware, and Trojan horses, but also malicious network intrusion and exploitation activities, such as identifying network backdoors and network scanning activities, and so-called “social engineering” activities, such as “phishing” exploits that seek usernames, passwords, social security numbers, or other personal information.

Opinions of the Office of Legal Counsel in Volume 33

from several sources, including commercial computer security services, publicly available computer security information, privately reported incidents to US-CERT, in-depth analysis by US-CERT analysts, and from other federal partners involved in computer defense. We understand that from information obtained through these sources, DHS will create signatures based upon known malicious computer code to guide the operations of EINSTEIN 2.0 sensors.

EINSTEIN 2.0 sensors will not scan actual Federal Systems Internet Traffic for malicious computer code as that traffic is in transmission, but instead will scan a temporary copy of that traffic created solely for the purpose of scanning by the sensors. The “original” Federal Systems Internet Traffic will continue to its destination without being scanned by EINSTEIN 2.0 sensors; thus, EINSTEIN 2.0 operations will not disrupt the normal operations of Federal Systems. But EINSTEIN 2.0 technology will create a temporary mirror image of all Federal Systems Internet Traffic of EINSTEIN 2.0 Participants for parallel scanning by the sensors. The temporary copy of Federal Systems Internet Traffic is created only for identifying known signatures. When EINSTEIN 2.0 sensors identify Federal Systems Internet Traffic containing packets with malicious computer code matching a signature, EINSTEIN 2.0 technology is designed to generate—in near-real time—an automated alert about the detected signature. The alert generally will not contain the content of the packet, but will include header information, such as the source or remote IP address associated with the traffic that generated the alert, metadata regarding the type of signature that was detected, and the date/time stamp.

In addition to generating automated alerts, EINSTEIN 2.0 operations will both acquire and store data packets from the mirror copy of Federal Systems Internet Traffic that are associated with a detected signature. Those packets, which may include the full content of Internet communications, such as e-mails, may be reviewed by analysts from US-CERT and other authorized persons involved in computer network defense. We understand that no packets other than those associated with a known signature will be acquired and stored. Accordingly, we understand that the vast majority of packets that are not associated with malicious computer code matching a signature will be deleted promptly. *See* Department of Homeland Security, *Privacy Impact Assessment for EINSTEIN 2*, at 12 (May 18, 2008) (stating that all “clean traffic” is promptly deleted).

We have been informed that EINSTEIN 2.0 operations are expected to improve substantially the Government’s ability to defend Federal Systems against intrusions and exploitations. EINSTEIN 2.0 operations will supplement—and not replace—the current individualized computer network security defenses of executive departments and agencies with a centralized and coordinated network defense system operated by DHS. That centralization and coordination of information regarding all Federal Systems Internet Traffic is expected to facilitate real-time situational awareness regarding malicious network activity across all Federal Systems. Improved situational awareness in turn will facilitate improved defensive measures, such as minimizing network vulnerabilities and alerting users of Federal Systems about particular malicious computer code detected against particular EINSTEIN 2.0 Participants. By sharing information throughout the Executive Branch regarding signatures detected in Federal Systems Internet Traffic, EINSTEIN 2.0 operations should facilitate improved defenses against known malicious computer code.

As part of enrolling in EINSTEIN 2.0 operations, each EINSTEIN 2.0 Participant is required to enter into a memorandum of agreement (“MOA”) with DHS. We understand that the MOA will require an EINSTEIN 2.0 Participant to certify that it has implemented procedures to provide appropriate notice to its employees that by using Government-owned information systems, the employee acknowledges and consents to the monitoring, interception, and search of his communications transiting through or stored on those systems, and that the employee has no reasonable expectation of privacy in his use of those systems.⁴ Those procedures are to include computer-user agreements, log-on banners, and computer-training programs. We understand that DHS must receive that certification from each EINSTEIN 2.0 Participant before any of the Participant’s Federal Systems Internet Traffic can be scanned by EINSTEIN 2.0 technology.

EINSTEIN 2.0 Participants will not be required to use a specific banner or user agreement. We have been advised that given the diversity of missions and organizations among departments and agencies within the Executive Branch and the varying technical constraints faced by those entities, there simply is no one-size-fits-all solution for providing notice to and obtaining the consent of employees for EINSTEIN 2.0 operations. We have been informed, however, that the MOA will include model log-on banner and model computer-user agreement language for EINSTEIN 2.0 Participants to consider in crafting their own banners and user agreements. The model language, which was developed by lawyers from DOJ with the input and advice of lawyers from DHS and other interested departments and agencies, is as follows:

- You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.
- Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.
- By using this information system, you understand and consent to the following:
 - You have no reasonable expectation of privacy regarding communications or data transiting or stored on this information system.
 - At any time, and for any lawful government purpose, the Government may monitor, intercept, and search any communication or data transiting or stored on this information system.
 - Any communications or data transiting or stored on this information system may be disclosed or used for any lawful government purpose.

[click button: I AGREE]

⁴ Throughout this memorandum we refer to “Executive Branch employees” and to the “employees” of EINSTEIN 2.0 Participants. By using the word “employees,” we do not mean to limit the requirement to provide appropriate notice and consent to only those persons in a common law employment relationship with the federal Government. Rather, the term “employees” in this memorandum should be understood to include “employees” as well as “officers,” “contractors,” and “agents” of EINSTEIN 2.0 Participants.

Opinions of the Office of Legal Counsel in Volume 33

The model computer-user agreement language contains the same substantive terms as the model log-on banner, except that it requires a computer user to sign a document indicating that the user “understand[s] and consent[s]” to the foregoing terms. Although we understand that EINSTEIN 2.0 Participants will not be required to use the exact model log-on banner and model computer-user agreement language, each EINSTEIN 2.0 Participant must certify that its log-on banners, computer-user agreements, and other computer policies contain language that demonstrates consent is “clearly given” and “clearly obtained” before EINSTEIN 2.0 becomes operational for the Participant’s Federal Systems Internet Traffic.⁵

DOJ has advised that with the consistent adoption, implementation, and enforcement of appropriate consent and notification procedures, EINSTEIN 2.0 operations would comply with the Fourth Amendment to the Constitution of the United States, the Wiretap Act, FISA, the SCA, and the Pen/Trap Act. The Department arrived at these conclusions after a lengthy review by the Office of the Deputy Attorney General, this Office, and, with respect to the statutes for which they have expertise, the National Security Division and the Computer Crimes and Intellectual Property Section of the Criminal Division. This memorandum explains the reasoning for those conclusions.

II.

We first explain the reasoning behind DOJ’s conclusion that the deployment, testing, and use of EINSTEIN 2.0 technology complies with the Fourth Amendment where each EINSTEIN 2.0 Participant consistently adopts and implements the model log-on banner or model computer-user agreement—or a log-on banner or computer-user agreement containing substantially equivalent terms establishing that the consent of its employees is “clearly given” and “clearly obtained.”

⁵ For example, DOJ already has in place a log-on banner that we believe would satisfy the MOA’s certification criteria. DOJ’s banner at present provides:

- You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.
- Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.
- By using this information system, you understand and consent to the following:
 - You have no reasonable expectation of privacy regarding any communications transmitted through or data stored on this information system.
 - At any time, the Government may monitor, intercept, search and/or seize data transiting or stored on this information system.
 - Any communications transmitted through or data stored on this information system may be disclosed or used for any U.S. Government-authorized purpose.

[click button: I AGREE]

A.

The Fourth Amendment provides in relevant part: “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.” U.S. Const. amend. IV. Government activity implicates the protections of the Fourth Amendment where it constitutes a “search” or a “seizure” within the meaning of the Fourth Amendment. The Supreme Court has said that a “search” occurs where the Government infringes upon a person’s legitimate expectation of privacy, consisting of both an actual, subjective expectation of privacy as well as an objectively reasonable expectation of privacy—“*i.e.*, one that has a source outside the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society.” *Minnesota v. Carter*, 525 U.S. 83, 88 (1998) (internal quotation marks omitted).

We think it plain that computer users exchanging Internet communications through Federal Systems lack a legitimate expectation of privacy in certain specific categories of data that will be subject to scanning by EINSTEIN 2.0 technology. There is no objectively reasonable expectation of privacy in information regarding the to/from addresses for e-mails, the IP addresses of Web sites visited, the total traffic volume of the user, and other addressing and routing information conveyed for the purpose of transmitting Internet communications to or from a user. See *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 904-05 (9th Cir. 2008); *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008); see also *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979) (no legitimate expectation of privacy in dialing, routing, addressing, and signaling information transmitted to telephone companies). E-mail addresses and IP addresses provide addressing and routing information to an Internet Service Provider (“ISP”) in the same manner as a telephone number provides switching information to a telephone company. *Forrester*, 512 F.3d at 510. Just as a telephone user has no objectively reasonable expectation of privacy in telephone numbers voluntarily turned over to the phone company to enable switching of a phone call, an Internet user has no such expectation of privacy in routing information submitted to an ISP in order to deliver an Internet communication. *Id.* That routing information also is akin to the addressing information written on the outside of a first-class letter, which also is not constitutionally protected. *Id.* at 511 (“E-mail, like physical mail, has an outside address ‘visible’ to the third-party carriers that transmit it to its intended location.”). With respect to information regarding the total volume of data received and transmitted by an Internet user, that information is no different from the information produced by a pen register regarding the number of incoming and outgoing calls at a particular phone number; and the Supreme Court has long held that an individual has no legitimate expectation of privacy in such information, which already has been exposed to a telecommunications carrier for the purpose of routing a communication. *Id.* Therefore, because there is no legitimate expectation of privacy with respect to the foregoing information transmitted for the purpose of routing Internet communications, the scanning of that information by EINSTEIN 2.0 technology does not constitute a “search” subject to the restrictions of the Fourth Amendment.

With respect to a user’s expectation of privacy in the content of an Internet communication (such as an e-mail), we assume for the purposes of this memorandum that a computer user generally has a legitimate expectation of privacy in that content while it is in

Opinions of the Office of Legal Counsel in Volume 33

transmission over the Internet. To date, the federal courts appear to agree that the sender of an e-mail, like the sender of a letter via first-class mail, has an objectively reasonable expectation of privacy in the content of a message while it is in transmission. *See, e.g., United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) (analogizing expectation of e-mail user in privacy of e-mail to expectation of individuals communicating by regular mail); *United States v. Maxwell*, 45 M.J. 406, 418 (C.A.A.F. 1996) (sender of an e-mail generally “enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant”); *see also Quon*, 529 F.3d at 905 (“[U]sers do have a reasonable expectation of privacy in the content of their text messages vis-à-vis the service provider.”).⁶

Here, EINSTEIN 2.0 technology will scan a mirror copy of the packet content of Federal Systems Internet Traffic—including packets that are part of e-mails—for malicious computer code associated with a signature while the e-mail is in transmission, and, thus, while a sender of the e-mail, we assume, generally retains an expectation of privacy in the content of that communication. Hence, the precise question for us is whether the Executive Branch’s automatic scanning of Federal Systems Internet Traffic for malicious computer code would implicate a computer user’s legitimate expectation of privacy in the content of his Internet communications. We consider the privacy expectations of two groups of computer users: (1) Executive Branch employees and (2) private individuals communicating with specific Executive Branch employees or with Executive Branch departments or agencies more generally.

1.

We first address the expectations of Executive Branch employees. The Supreme Court has rejected the contention that public employees “can never have a reasonable expectation of privacy in their place of work.” *O’Connor v. Ortega*, 480 U.S. 709, 717 (1987) (plurality); *id.* at 729-31 (Scalia, J., concurring). “Individuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer.” *Id.* at 717 (plurality). Nevertheless, there are reasons to doubt that an Executive Branch employee has a legitimate expectation of privacy in the content of his Internet communications made using Government-owned information systems. The text of the Fourth Amendment protects the right of the people to be secure only in “*their* persons, houses, papers, and effects.” U.S. Const. amend. IV (emphasis added). Although an individual generally possesses a legitimate expectation of privacy in his own personal computer, *e.g., United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007); *Lifshitz*, 369 F.3d at 190, it is less clear that an Executive Branch employee has a

⁶ It also appears that the federal courts agree that, again like the sender of a first-class letter, an individual has a “diminished” expectation of privacy in the content of an e-mail that “ha[s] already arrived at the recipient.” *Lifshitz*, 369 F.3d at 190 (internal citations omitted); *see Guest v. Leis*, 225 F.3d 325, 333 (6th Cir. 2001) (individual does not have a reasonable expectation of privacy “in an e-mail that had already reached its recipient; at this moment, the e-mailer would be analogous to a letter-writer, whose expectation of privacy ordinarily terminates upon delivery of the letter”); *Maxwell*, 45 M.J. at 417 (once an e-mail, like a letter, “is received and opened, the destiny of the [e-mail] then lies in the control of the recipient . . . , not the sender”); *United States v. Jones*, No. 03-15131, 149 Fed. Appx. 954, 959 (11th Cir. Sept. 20, 2005) (unpublished) (“We have not addressed previously the existence of a legitimate expectation of privacy in text messages or e-mails. Those circuits that have addressed the question have compared e-mails with letters sent by postal mail. Although letters are protected by the Fourth Amendment, ‘if a letter is sent to another, the sender’s expectation of privacy ordinarily terminates upon delivery.’”) (quoting *United States v. King*, 55 F.3d 1193, 1195-96 (6th Cir. 1995)).

legitimate expectation of privacy in Internet communications he makes using a computer that is the property of the United States Government, provided by the taxpayers for his use at work. *Cf. Muick v. Glenayre Elecs.*, 280 F.3d 741, 743 (7th Cir. 2002) (Posner, J.) (employee “had no right of privacy in the computer that [his private employer] had lent him for use in the workplace”); *but cf. United States v. Slanina*, 283 F.3d 670, 677 (5th Cir. 2002) (employee had reasonable expectation of privacy in use of city-owned computer where there was no “city policy placing Slanina on notice that his computer usage would be monitored” and there was no “indication that other employees had routine access to his computer”), *vacated on other grounds*, 537 U.S. 802 (2002). A government employee lacks an ownership or other property interest in the computer he uses at work; and he especially lacks any such interests in the Federal Systems—the network infrastructure that the Government provides to enable its employees to access the Internet—that, unlike his personal computer, ordinarily is not within his day to day control.

As a general matter, however, the Supreme Court has held that there may be circumstances in which a government employee has a legitimate expectation of privacy in the contents of governmental property that the employee uses or controls at work, such as an office or a locked desk drawer. *See O’Connor*, 480 U.S. at 716-19 (1987) (plurality) (public employee has a reasonable expectation of privacy in personal items, papers, and effects in office, desk, and file cabinets provided by public employer); *see id.* at 730-31 (Scalia, J., concurring) (government employee has a legitimate expectation of privacy in the contents of his office). And the Court also has made it clear that property interests are not conclusive regarding the legitimacy of an individual’s expectation of privacy. *See Oliver v. United States*, 466 U.S. 170, 183 (1984) (“The existence of a property right is but one element in determining whether expectations of privacy are legitimate.”); *Warden v. Hayden*, 387 U.S. 294, 304 (1967) (“The premise that property interests control the right of the Government to search and seize has been discredited.”); *see also Legality of Television Surveillance in Government Offices*, 3 Op. O.L.C. 64, 66-67 (1979) (government ownership of office insufficient to establish employee’s lack of expectation of privacy where “in a practical sense” the employee exercises exclusive use of the office) (“*Television Surveillance Opinion*”); *but cf. United States v. Ziegler*, 474 F.3d 1184, 1191 (9th Cir. 2007) (private employee’s “workplace computer . . . is quite different from the” property described in *O’Connor*, because the computer was owned by the company, was controlled jointly by the company and the employee, and was monitored to ensure that employees did not visit pornographic or other inappropriate Web sites).

Instead, whether, in a particular circumstance, a government employee has a legitimate expectation of privacy in his use of governmental property at work is determined by “[t]he operational realities of the workplace” and “by virtue of actual office practices and procedures, or by legitimate regulation.” *O’Connor*, 480 U.S. at 717 (plurality); *see United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000) (“[O]ffice practices, procedures, or regulations may reduce legitimate privacy expectations.”). Here, we believe that an Executive Branch employee will not have a legitimate expectation of privacy in the content of his Internet communications transmitted over Government-owned information systems, provided that EINSTEIN 2.0 Participants consistently adopt, implement, and enforce appropriate consent and notification procedures, such as the model log-on banner or model computer-user agreement.

Opinions of the Office of Legal Counsel in Volume 33

Although the Supreme Court has not addressed the issue, the federal courts of appeals have held that the use of log-on banners or computer-user agreements, such as the models provided by DHS to EINSTEIN 2.0 Participants, can eliminate any legitimate expectation of privacy in the content of Internet communications made at work using Government-owned information systems. For example, in *United States v. Simons*, the computer-use policy at the Foreign Bureau of Information Services (“FBIS”), a division of the Central Intelligence Agency, expressly noted that FBIS would “‘audit, inspect, and/or monitor’” employees’ use of the Internet, “including all file transfers, all websites visited, and all e-mail messages, ‘as deemed appropriate.’” 206 F.3d at 398 (quoting policy). The Fourth Circuit held that this policy “placed employees on notice that they could not reasonably expect that their Internet activity would be private” and that, “in light of the Internet policy, Simons lacked a legitimate expectation of privacy” in his use of the Internet at work. *Id.*

Likewise, in *United States v. Angevine*, 281 F.3d 1130 (10th Cir. 2002), the Tenth Circuit held that a professor at a state university had no reasonable expectation of privacy in his Internet use in light of a broadly worded computer-use policy and log-on banner. The computer-use policy stated that the university “‘reserves the right to view or scan any file or software stored on the computer or passing through the network, and will do so periodically’” and has “‘a right of access to the contents of stored computing information at any time for any purpose which it has a legitimate need to know.’” *Id.* at 1133 (quoting policy). The log-on banner provided that “‘all electronic mail messages . . . contain no right of privacy or confidentiality except where Oklahoma or Federal statutes expressly provide for such status,’” and that the university may “‘inspect electronic mail usage by any person at any time without prior notice as deemed necessary to protect business-related concerns . . . to the full extent not expressly prohibited by applicable statutes.’” *Id.* (quoting banner). The court held that these notices prevent university employees “from reasonably expecting privacy in data downloaded from the Internet onto [u]niversity computers,” because users are warned that data “is not confidential either in transit or in storage” and that “network administrators and others were free to view data downloaded from the Internet.” *Id.* at 1134.

The Eighth Circuit came to the same conclusion in *United States v. Thorn*, 375 F.3d 679 (8th Cir. 2004), *vacated on other grounds*, 543 U.S. 1112 (2005). In *Thorn*, a state employee had acknowledged in writing a computer-use policy, which warned that employees “‘do not have any personal privacy rights regarding their use of [the agency’s] information systems and technology. An employee’s use of [the agency’s] information systems and technology indicates that the employee understands and consents to [the agency’s] right to inspect and audit all such use as described in this policy.’” *Id.* at 682 (quoting policy). As a result of this policy, the court held that the state employee “did not have any legitimate expectation of privacy with respect to the use and contents of his [work] computer,” because under the agency’s policy, employees have “no personal right of privacy with respect to their use of the agency’s computers” and provides the state with a “right to access all of the agency’s computers.” *Id.* at 683.

The decisions of other federal courts that have addressed the issue support the proposition that actual and consistent use of log-on banners or computer-user agreements can eliminate any legitimate expectation of an employee in the privacy with respect to his Internet communications using Government-owned information systems. *See Bibby v. Board of Regents*, 419 F.3d 845,

850-51 (8th Cir. 2005) (university computer policy warning user “not to expect privacy if the university has a legitimate reason to conduct a search” and that “computer files, including e-mail, can be searched” under certain conditions eliminates any reasonable expectation of privacy the use of the computer network); *Muick*, 280 F.3d at 743 (employer’s announced policy of inspecting work computers “destroyed any reasonable expectation of privacy”); *United States v. Monroe*, 52 M.J. 326, 330 (C.A.A.F. 1999) (no reasonable expectation of privacy that network administrators would not review e-mail where banner stated that “users logging on to this system consent to monitoring”); *see also Heckenkamp*, 482 F.3d at 1147 (“[P]rivacy expectations may be reduced if the user is advised that information transmitted through the network is not confidential and that the systems administrators may monitor communications transmitted by the user.”) (citing *Angevine*, 281 F.3d at 1134, and *Simons*, 206 F.3d at 398); *cf. Slanina*, 283 F.3d at 677 (“[G]iven the absence of a city policy placing Slanina on notice that his computer usage would be monitored and the lack of any indication that other employees had routine access to his computer, we hold that Slanina’s expectation of privacy was reasonable.”); *Leventhal v. Knappek*, 266 F.3d 64, 73-74 (2d Cir. 2001) (public employee had reasonable expectation of privacy in the contents of his office computer because his employer neither “had a general practice of routinely conducting searches of office computers” nor “had placed [him] on notice that he should have no expectation of privacy in the contents of his office computer”).

In light of these decisions, we believe that an Executive Branch employee who has clicked through the model log-on banner or signed the model computer-user agreement—or a log-on banner or computer-user agreement containing substantially equivalent terms—would not have a legitimate expectation of privacy in the contents of Internet communications made using Government-owned information systems and transmitted over Federal Systems. The model log-on banner is explicit and comprehensive regarding an employee’s lack of a legitimate expectation of privacy in his use of Government-owned information systems. That banner states that the information system the employee uses is the property of the Government and “is provided for U.S. Government-authorized use only.” The user “understand[s] and consent[s]” that: he has “no reasonable expectation of privacy regarding communications or data transiting or stored” on that information system; “[a]t any time, and for any lawful government purpose, the Government may monitor, intercept, and search any communication or data transiting or stored” on the information system; and any communications transmitted through or data stored on the information system “may be disclosed or used for any lawful government purpose.” *See supra* pp. 5-6. We believe that the current DOJ banner, which deviates from the model log-on banner and the model computer-user agreement language in some respects, is to the same effect. *See supra* n. 5. Both the model log-on banner and computer-user agreement and the current DOJ log-on banner are at least as robust as—and we think they are even stronger than—the materials that eliminated an employee’s legitimate expectation of privacy in the content of Internet communications in *Simons*, *Angevine*, *Thorn*, *Biby*, and *Monroe*. Therefore, we believe that adoption of the language in those model materials by EINSTEIN 2.0 Participants would eliminate their employees’ legitimate expectations of privacy in their uses of Government-owned information systems with respect to the lawful government purpose of protecting Federal Systems against network intrusions and exploitations.

It is important to note, however, that the use of log-on banners or computer-user agreements may not be sufficient to eliminate an employee’s legitimate expectation of privacy if

Opinions of the Office of Legal Counsel in Volume 33

the statements and actions of Executive Branch officials contradict these materials. Recently, in *Quon v. Arch Wireless Operating Company*, the Ninth Circuit held that a police officer had a legitimate expectation of privacy in the contents of text messages sent and received on his department-provided pager notwithstanding departmental policies, because informal guidance from the officer's superiors had established, in practice, that the department would not monitor the content of his text messages. *See* 529 F.3d at 906-07. Thus, the "operational reality" at the department established a reasonable expectation of privacy in the text messages sent through a department-provided pager. *Id.* at 907 (quoting *O'Connor*, 480 U.S. at 717). In light of *Quon*, management officials at EINSTEIN 2.0 Participants should be careful not to make statements—either formal or informal—or to adopt practices that contradict the clear position in a log-on banner or a computer-user agreement that an employee has no legitimate expectation of privacy in his use of Government-owned information systems.

2.

We next consider whether an individual in the private sector communicating with an Executive Branch employee (such as where an individual sends an e-mail to either the employee's governmental—i.e., work—or personal e-mail account) or with an EINSTEIN 2.0 Participant directly (such as where an individual browses the Web site of the participating department or agency) has a legitimate expectation of privacy in the content of those communications. We conclude that he does not, provided that EINSTEIN 2.0 Participants consistently adopt, implement, and enforce notice and consent procedures for Executive Branch employees, such as the model log-on banner or model computer-user agreement, or banners or user agreements with terms that are substantially equivalent to those models.

The Supreme Court has held repeatedly that "[t]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *United States v. Miller*, 425 U.S. 435, 443 (1976); *see SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984) ("[W]hen a person communicates to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information or records thereof to law enforcement authorities."); *Smith*, 442 U.S. at 743-44 ("[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."). Accordingly, "[i]t is well[] settled" that where a person "reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information." *United States v. Jacobsen*, 466 U.S. 109, 117 (1984).

We believe this principle applies to a person e-mailing an Executive Branch employee at the employee's personal e-mail account, where the employee has agreed to permit the Government to monitor, intercept, and search all of his Internet communications and data transiting Government-owned information systems. By clicking through the model log-on banner or agreeing to the terms of the model computer-user agreement, an Executive Branch employee gives *ex ante* permission to the Government to intercept, monitor, and search "any communications" and "any data" transiting or stored on a Government-owned information

system for any “lawful purpose.” That permission necessarily includes the interception, monitoring, and searching of all personal communications and data sent or received by an employee using that system for the purpose of protecting Federal Systems against malicious network activity.⁷ Therefore, an individual who communicates with an employee who has agreed to permit the government to intercept, monitor, and search any personal use of the employee’s Government-owned information systems has no Fourth Amendment right to prohibit the Government from doing what the employee has authorized. *See Jerry T. O’Brien, Inc.*, 467 U.S. at 743; *Jacobsen*, 466 U.S. at 117; *Miller*, 425 U.S. at 443.

This well-settled Fourth Amendment principle applies even where, for example, the sender of an e-mail to an employee’s personal, Web-based e-mail account (such as Gmail or Hotmail) does not know of the recipient’s status as a federal employee or does not anticipate that the employee might read an e-mail sent to a personal e-mail account at work. Indeed, it is well established that a person communicating with another (who turns out to be an agent for the government) assumes the risk that the person has agreed to permit the Government to monitor the contents of that communication. *See, e.g., United States v. White*, 401 U.S. 745, 749-51 (1971) (plurality opinion) (no Fourth Amendment protection against government monitoring of communications through transmitter worn by undercover operative); *Hoffa v. United States*, 385 U.S. 293, 300-03 (1966) (information disclosed to individual who turns out to be a government informant is not protected by the Fourth Amendment); *Lopez v. United States*, 373 U.S. 427, 439 (1963) (same); *Rathbun v. United States*, 355 U.S. 107, 111 (1957) (“Each party to a telephone conversation takes the risk that the other party may have an extension telephone and may allow another to overhear the conversation. When such takes place there has been no violation of any privacy of which the parties may complain.”); *United States v. Coven*, 662 F.2d 162, 173-74 (2d Cir. 1981) (individual has no expectation of privacy in documents given to or accessible by undercover informant). Therefore, where an employee agrees to let the Government intercept, monitor, and search any communication or data sent, received, or stored by a Government-owned information system, the Government’s interception of the employee’s Internet communications with individuals outside the Executive Branch does not infringe upon those individuals’ legitimate expectations of privacy. *See also infra* pp. 16-21 (consent of employee).

We also think it clear that an individual submitting information directly to an EINSTEIN 2.0 Participant through the Internet—such as where an individual submits an application online or browses the public Web site of the Participant—has no legitimate expectation of privacy in

⁷ The language of the model log-on banner and model computer-user agreement unambiguously applies to “any” communications and “any” data transiting through or stored on a Government-owned information system and clearly eliminates any reasonable expectation of privacy that a user could have with respect to such communications and data. Nevertheless, if a participating department or agency wished to add even more express notice that those terms apply to personal communications and personal data that an employee sends, receives, or stores using a Government-owned information system, such as the use of personal Web-based e-mail accounts at work, the department or agency could so in several ways. To be clear, we do not believe that any such efforts are legally required. But should a participating department or agency decide to go even further than the robust protection afforded by the model language, it would have several options at its disposal. For example, the department or agency could include in its log-on banner or computer-user agreement express language regarding personal communications or data. Or it could notify employees through computer training and certification programs that *any* personal use of Government-owned information systems by an employee is subject to interception, monitoring, and searching.

Opinions of the Office of Legal Counsel in Volume 33

the contents of any information that he transmits to the department or agency. An individual has no expectation of privacy in communications he makes to a known representative of the Government. See *United States v. Caceres*, 440 U.S. 741, 750-51 (1979) (individual has no reasonable expectation of privacy in communications with IRS agent made in the course of an audit); cf. *Transmission by a Wireless Carrier of Information Regarding a Cellular Phone User's Physical Location to Public Safety Organizations*, 20 Op. O.L.C. 315, 321 (1996) (individual calling 911 lacks a reasonable expectation that information regarding his location will not be transmitted to public safety organizations) (“*Caller ID Opinion*”). Furthermore, an individual who communicates information to another individual who turns out to be an undercover agent of the Government has no legitimate expectation of privacy in the content of that information. See *supra* p. 13. *A fortiori*, where an individual is communicating with a *declared* agent of the Government—here, an executive department or agency—the individual does not have a legitimate expectation that his communication would not be monitored or acquired by the Government. It also is well established that an individual does not have any legitimate expectation of privacy in information that he reveals to a third party. See *supra* p. 12; see also *United States v. Ganoë*, 538 F.3d 1117, 1127 (9th Cir. 2008) (individual has no legitimate expectation of privacy in computer files he made accessible to others); *United States v. King*, 509 F.3d 1338, 1342 (11th Cir. 2007) (individual has no legitimate expectation of privacy in computer files shared with others over network on military base). Hence, an individual could not possibly have a legitimate expectation of privacy in communications he shares directly with a department or agency of the Government. Indeed, the entire purpose of his online communication is for the Government to receive the content of his message. Cf. *Caller ID Opinion*, 20 Op. O.L.C. at 321 (purpose of calling 911 is to request governmental aid in an emergency). Therefore, we also do not believe that EINSTEIN 2.0 operations implicate a legitimate expectation of privacy in the content of Internet communications made between private individuals and an EINSTEIN 2.0 Participant.

B.

Even if EINSTEIN 2.0 operations were to constitute a “search” under the Fourth Amendment, we believe that those operations nonetheless would be consistent with that Amendment’s “central requirement” that all searches be *reasonable*. *Illinois v. McArthur*, 531 U.S. 326, 330 (2001) (internal quotation marks omitted). Where, as here, the statutes and common law of the founding era do not provide a specific analogue, we analyze the reasonableness of a search in light of traditional judicial standards, balancing the degree of intrusion upon an individual’s privacy in light of the search’s promotion of legitimate governmental interests. *Virginia v. Moore*, 128 S. Ct. 1598, 1602-04 (2008). In many circumstances, a search is unreasonable unless law enforcement officials first obtain a warrant “issued by a neutral magistrate after finding probable cause.” *McArthur*, 531 U.S. at 330. Yet the Supreme Court also has “made it clear that there are exceptions to the warrant requirement,” *id.*, and that “neither a warrant nor probable cause, nor, indeed, any measure of individualized suspicion, is an indispensable component of reasonableness in every circumstance,” *National Treasury Employees Union v. Von Raab*, 489 U.S. 656, 665 (1989).

One well-known exception to the need to obtain a warrant based upon probable cause is where a person consents to the search. See *Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973)

(consent is “one of the specifically established exceptions to the requirements of both a warrant and probable cause”). An Executive Branch employee who clicks “I agree” in response to the model log-on banner, enabling him to use Government-owned information systems to access the Internet, or an employee who signs the model computer-user agreement, thereby acknowledging his “consent[]” to monitoring of his use of those systems, certainly appears to have consented expressly to the scanning of his incoming and outgoing Internet communications.

In the context of public employment, however, merely obtaining the consent of an employee to search is not necessarily coextensive with the requirements of the Fourth Amendment. Such consent must be voluntary and cannot be obtained through duress or coercion. *See generally Schneekloth*, 412 U.S. at 223-35. Where an employee is confronted with the choice of either consenting to a search or facing adverse employment consequences, it is debatable whether consent is in fact voluntary. An Executive Branch employee who refuses to accept a log-on banner or to sign a computer-user agreement likely will not be able to access his computer and, hence, may be unable to perform his duties. *See, e.g., Anobile v. Pelligrino*, 303 F.3d 107, 124 (2d Cir. 2002) (“[C]oercion may be found where one is given a choice between one’s employment and one’s constitutional rights.”).

Indeed, putting a public employee to the choice of either consenting to an *unreasonable* search or facing potential adverse employment consequences may impose an invalid condition on public employment. Into the first part of the 20th Century, the Government “enjoyed plenary authority to condition public employment on the employee’s acceptance of almost any term of employment including terms that restricted constitutional rights.” Memorandum for the Attorney General, from Charles J. Cooper, Assistant Attorney General, Office of Legal Counsel, *Re: The Legality of Drug Testing Programs for Federal Employees* at 4 (Aug. 25, 1986) (“*Drug Testing Opinion*”). That view has since given way to the doctrine of unconstitutional conditions, which, as applied to public employment, prohibits the Government from conditioning employment on the relinquishment of a constitutional right, such as the First Amendment right to freedom of speech. *See, e.g., Pickering v. Board of Educ.*, 391 U.S. 563, 568 (1968) (“The theory that public employment, which may be denied altogether may be subjected to any conditions, regardless of how unreasonable, has been uniformly rejected.”) (quoting *Keyishian v. Board of Regents*, 385 U.S. 589, 605-06 (1967)). More than 20 years ago, we noted that the federal courts of appeals “have generally applied the doctrine of unconstitutional conditions” to conditions of employment that would require government employees to forgo their Fourth Amendment rights against unreasonable searches. *Drug Testing Opinion* at 7 (“[T]here appears to be a consensus that the doctrine of unconstitutional conditions applies in the Fourth Amendment context.”). That statement is just as true today. *See, e.g., Anobile*, 303 F.3d at 123-25 (search of dormitories of horse-racing industry employees’ pursuant to their written consent unreasonable under the Fourth Amendment); *McGann v. Northeast Ill. Reg’l Commuter R.R. Corp.*, 8 F.3d 1174, 1180 (7th Cir. 1993) (“[T]he conditioning of access on the surrender of one’s Fourth Amendment rights raises the specter of an unconstitutional condition.”); *McDonell v. Hunter*, 807 F.2d 1302, 1310 (8th Cir. 1987) (“If a search is unreasonable, a government employer cannot require that its employees consent to that search as a condition of employment.”); *Doyon v. Home Depot U.S.A., Inc.*, 850 F. Supp. 125, 129 (D. Conn. 1994) (Cabrane, J.) (“[C]onsent to an unreasonable search is not voluntary when required as a condition of employment.”).

Opinions of the Office of Legal Counsel in Volume 33

We do not believe, however, that the unconstitutional conditions doctrine applies here, because obtaining the consent of employees for EINSTEIN 2.0 operations does not require Executive Branch employees to consent to an *unreasonable* search. Notwithstanding that the terms of both the model log-on banner and the model computer-user agreement would permit monitoring of an employee's computer use for purposes other than network defense, we believe that the specific EINSTEIN 2.0 operations to which Executive Branch employees would be asked to consent would be reasonable.⁸ Where, as here, an Executive Branch employee is being asked to consent only to a reasonable search, there is no invalid conditioning of public employment on the employee's relinquishment of his Fourth Amendment rights against unreasonable searches and no coercion that renders a search involuntary. *See, e.g., United States v. Sihler*, 562 F.2d 349 (5th Cir. 1977) (prison employee's consent to routine search of his lunch bag valid); *cf. Drug Testing Opinion* at 7 (“[C]onsent to an *unreasonable* search is invalid.”) (emphasis added); *Anobile*, 303 F.3d at 124 (similar); *McDonnell*, 807 F.2d at 1310 (similar). Thus, the inquiry regarding the voluntariness of an Executive Branch employee's consent merges with the underlying inquiry regarding the overall reasonableness of EINSTEIN 2.0 operations.⁹ *See Drug Testing Opinion* at 7 (“[I]t appears that the government could not insist upon a complete waiver of Fourth Amendment rights as a condition of public employment and that the courts will scrutinize the search under the Fourth Amendment to determine whether it is reasonable.”).

Therefore, we turn to the reasonableness of EINSTEIN 2.0 operations. A work-related administrative search by a public employer conducted for a non-law enforcement purpose is not *per se* unreasonable under the Fourth Amendment simply because the Government has not obtained a warrant based upon probable cause. The Supreme Court has said that “special needs, beyond the normal need for law enforcement,” may render the warrant and probable cause provisions of the Fourth Amendment “impracticable for legitimate work-related, non-investigatory intrusions as well as investigations of work-related misconduct.” *O'Connor*, 480 U.S. at 725 (plurality) (internal quotation marks and citations omitted); *id.* at 732 (Scalia, J., concurring) (searches in the government-employment context present “special needs”); *see also National Treasury Employees Union*, 489 U.S. at 665-66 (warrant and probable cause provisions of the Fourth Amendment are inapplicable to a search that “serves special governmental needs, beyond the normal need for law enforcement”); *Griffin v. Wisconsin*, 483 U.S. 868, 872 (1987) (special needs doctrine applies in circumstances that make the “warrant and probable cause requirement impracticable”). Rather, “public employer intrusions on the constitutionally protected privacy interests of government employees for noninvestigatory, work-related purposes

⁸ Because the question presented to us is whether an employee's consent to conduct the particular scanning activities performed by EINSTEIN 2.0 technology would be valid under the Fourth Amendment, we do not address whether there would be valid consent to conduct any other search that could be conducted pursuant to the terms of the model log-on banner or the model computer-user agreement. *See Warshak v. United States*, 532 F.3d 521, 529-31 (6th Cir. 2008) (en banc) (rejecting premature Fourth Amendment challenge to facial constitutionality of provisions of the Stored Communications Act).

⁹ Indeed, the consent of an employee is one factor the courts consider in determining whether a search by a public employer is reasonable. *See, e.g., National Treasury Employees Union*, 489 U.S. at 672 & n.2 (considering consent to drug testing by Customs officers as one factor in concluding that such testing was reasonable); *United States v. Scott*, 450 F.3d 863, 868 (9th Cir. 2006) (“[S]earches of government employees still must be reasonable. . . . The employee's assent is merely a relevant factor in determining how strong his expectation of privacy is, and thus may contribute to a finding of reasonableness.”) (internal citations omitted).

... should be judged by the standard of reasonableness under all the circumstances.” *O’Connor*, 480 U.S. at 726 (plurality); *see id.* at 732 (Scalia, J., concurring).

Here, the Government plainly has a lawful, work-related, noninvestigatory purpose for the use of EINSTEIN 2.0’s intrusion-detection system, namely the protection of Federal Systems against unauthorized network intrusions and exploitations. *See Heckenkamp*, 482 F.3d at 1148 (preventing misuse of and damage to university computer network is a lawful purpose); *see also National Treasury Employees Union*, 489 U.S. at 668 (special needs include government’s need to “discover . . . latent or hidden” hazards); Federal Information Security Management Act of 2002, Public Law No. 107-347, § 301, 44 U.S.C. §§ 3541-3549 (2006) (“FISMA”) (establishing purposes and authorities for the protection of federal information systems). As we have already noted, *see supra* p. 2, there is a substantial history of intrusions and exploitations against Federal Systems. The deployment of EINSTEIN 2.0 technology is designed to provide greater awareness regarding intrusions and exploitations against those Systems in order to facilitate improved network defenses against malicious network activity. Those goals are unrelated to the needs of ordinary criminal law enforcement. *See Heckenkamp*, 482 F.3d at 1147-48 (state university has “separate security interests” in maintaining integrity and security of its network that are unrelated to interest in law enforcement); *see also Illinois v. Lidster*, 540 U.S. 419, 424 (2004) (although ordinary law enforcement objectives do not qualify as “special needs,” certain distinct “special law enforcement concerns” do); *Michigan Dep’t of State Police v. Sitz*, 496 U.S. 444 (1990) (upholding highway checkpoint stops designed to detect and prevent drunk driving). It is true that DHS may share alerts of detected signatures associated with malicious computer code with other executive departments and agencies, including law enforcement agencies, as permitted by applicable law and DHS procedures. The disclosure of alert information to law enforcement agencies, however, is at most an ancillary, rather than a central, feature of EINSTEIN 2.0 operations. *Cf. Ferguson v. City of Charleston*, 532 U.S. 67, 79-80 (2001) (“central and indispensable feature” of hospital policy to screen obstetrics patients for cocaine was to facilitate “the use of law enforcement” tools—arrest and prosecution—“to coerce the patients into substance abuse treatment”); *City of Indianapolis v. Edmond*, 531 U.S. 32, 44 (2001) (“primary purpose” of narcotics checkpoints is to advance the “general interest” in “ordinary crime control”). We understand that EINSTEIN 2.0 operations are for the purpose of protecting Federal Systems, *see supra* pp. 4-5, and are not conducted in order to advance ordinary law enforcement goals. Therefore, we conclude that EINSTEIN 2.0 operations would advance special governmental needs distinct from the ordinary interest in criminal law enforcement.

Furthermore, it would be impracticable to require the Government to obtain a warrant based upon probable cause before deploying EINSTEIN 2.0 technology to detect malicious cyber activity against Federal Systems. The need for coordinated situational awareness regarding all intrusions and exploitations against Federal Systems is inconsistent with the requirement to obtain a warrant based upon probable cause. *See Board of Educ. v. Earls*, 536 U.S. 822, 828 (2002) (warrant and probable cause requirements are “peculiarly related to criminal investigations and may be unsuited to determining the reasonableness of administrative searches where the Government seeks to prevent the development of hazardous conditions”). Indeed, the goal of near-real time awareness of malicious network activity is incompatible with a requirement to obtain a warrant. Given the constant stream of intrusions and exploitations

Opinions of the Office of Legal Counsel in Volume 33

against Federal Systems and the time it would take to seek and obtain a warrant, it would be entirely impracticable—if not impossible—to identify data packets containing malicious code in near real-time if the Government was required first to obtain a warrant before each such action. *See Skinner*, 489 U.S. at 623 (interest in dispensing with warrant requirement is at its strongest where “the burden of obtaining a warrant is likely to frustrate the governmental purpose behind the search”) (internal quotation marks omitted). Requiring a particularized warrant based upon probable cause before a scan for each signature would introduce an element of delay, thus frustrating the Government’s ability to collect information regarding intrusions and exploitations in a timely manner. *See Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995) (obtaining a warrant based upon probable cause is not a necessary element of reasonableness where such a requirement “would unduly interfere with the swift and informal” procedures needed to facilitate the government’s special needs) (internal quotation marks omitted). Moreover, in light of the speed and frequency with which intrusion and exploitation techniques change, requiring the Government to obtain a warrant to use EINSTEIN 2.0 sensors to protect Federal Systems would require nearly continuous, ongoing, daily supervision by the courts of the details of the Government’s network-defense activities. Such supervision would frustrate efforts to protect Federal Systems and to obtain new information regarding advanced intrusion and exploitation techniques. *See Heckenkamp*, 482 F.3d at 1148 (“[R]equiring a warrant to investigate potential misuse of the university’s computer network would disrupt the operation of the university and the network that it relies upon in order to function.”). For these reasons, we do not believe that EINSTEIN 2.0 operations would be presumptively unreasonable absent a warrant justified by probable cause.

Therefore, the reasonableness of EINSTEIN 2.0 operations is measured in light of the “totality of the circumstances,” *United States v. Knights*, 534 U.S. 112, 118 (2001), in “the context within which a search takes place,” *New Jersey v. T.L.O.*, 469 U.S. 325, 337 (1985). In the context of a workplace search by a public employer, the reasonableness analysis requires balancing the “invasion of the employees’ legitimate expectation of privacy against the government’s need for supervision, control, and the efficient operation of the workplace.” *O’Connor*, 480 U.S. at 719-20 (plurality); *see Knights*, 534 U.S. at 118-19 (reasonableness inquiry balances, “on the one hand, the degree to which it intrudes upon an individual’s privacy and, on the other, the degree to which a search is needed for the promotion of legitimate governmental interests”) (internal quotation marks omitted). A reasonable workplace search must be “justified at its inception” and “reasonably related in scope to the circumstances which justified the interference in the first place.” *O’Connor*, 480 U.S. at 726 (plurality) (internal quotation marks omitted).

Based upon the information available to us, we believe that EINSTEIN 2.0 operations are reasonable under the totality of the circumstances. In light of the substantial history of intrusions and exploitations against Federal Systems, *see supra* p. 2, the deployment and use of EINSTEIN 2.0 technology to scan Federal Systems Internet Traffic of EINSTEIN 2.0 Participants for malicious computer code certainly is “justified at its inception.” *O’Connor*, 480 U.S. at 726 (plurality) (internal quotation marks omitted).

We also conclude that any search conducted under EINSTEIN 2.0 operations would have a minimal impact upon the legitimate privacy expectations of computer users. The Supreme

Court has said that “[w]hen faced with . . . diminished expectations of privacy, minimal intrusions, or the like, certain general, or individual, circumstances may render a warrantless search or seizure reasonable.” *McArthur*, 531 U.S. at 330. We already have noted that individuals have no legitimate expectation of privacy whatsoever in certain categories of information collected by EINSTEIN 2.0—e.g., to/from addresses for e-mails, the IP addresses of Web sites visited, and the total traffic volume of a user—generated in connection with the routing of Internet communications. *See supra* pp. 7-8. And in light of the notice and consent procedures that EINSTEIN 2.0 Participants must adopt under the MOA, we believe that an individual’s expectation of privacy in the content of Internet communications transiting Federal Systems would, at a minimum, be significantly diminished. *See supra* pp. 10-14. Furthermore, we think it is reasonably likely that most Executive Branch employees and United States persons interacting with EINSTEIN 2.0 Participants and their employees neither intend to include nor want to receive malicious computer code in their e-mails and other Internet communications. And those who do intentionally unleash malicious computer code upon the Internet in order to conduct an unauthorized exploitation against Federal Systems have “no reasonable expectation of privacy” in the contents of those unauthorized Internet communications. 18 U.S.C. § 2510(21)(A).

We also conclude that the use of EINSTEIN 2.0 technology to detect malicious computer code in Federal Systems Internet Traffic imposes, at worst, a minimal burden upon legitimate privacy rights. Indeed, we understand that the actual scope of content monitoring by EINSTEIN 2.0 technology will be quite narrow. EINSTEIN 2.0 technology scans a mirror copy of the Federal Systems Internet Traffic of EINSTEIN 2.0 Participants. Of course, the EINSTEIN 2.0 technology will scan a copy of every single data packet of the Federal Systems Internet Traffic of those Participants. But we understand that the technology will scan that traffic—and only that traffic—only for particular malicious computer code associated with specific signatures. There is no authorization to acquire the content of any communication unrelated to detecting malicious computer code present in the packet. Therefore, we believe the intrusion upon any expectation of privacy in the privacy of the content of Internet communications that computer users may have vis-à-vis EINSTEIN 2.0 operations would be minimal, encompassing only the intrusion of searching for specified malicious computer code.

Our conclusion finds some support in the Supreme Court’s cases holding that a search technique that reveals only unlawful activity is not subject to the Fourth Amendment at all. *See Jacobsen*, 466 U.S. at 123-24 (chemical field test that could disclose only whether white powder was cocaine does not infringe upon a legitimate expectation of privacy); *see also United States v. Place*, 462 U.S. 696, 706-07 (1983) (canine sniff by a well-trained narcotics detection dog that discloses only the present or absence of narcotics is “*sui generis*” because it “is so limited both in the manner in which the information is obtained and in the content of the information revealed by the procedure” and, therefore, does not intrude upon a legitimate expectation of privacy). The inclusion of malicious computer code in an e-mail or other Internet-based communication may or may not be analogous to the possession of contraband, such as narcotics, at issue in *Jacobsen* and *Place*. But the use of malicious computer code to gain access to Federal Systems is a federal offense, *see, e.g.*, 18 U.S.C. § 1030(a)(2)(B), (3), & (5)(A) (2006), and the inclusion of that code in, for example, an e-mail is far from “perfectly lawful activity,” *Illinois v. Caballes*, 543 U.S.

Opinions of the Office of Legal Counsel in Volume 33

405, 409-10 (2005) (emphasizing that a canine sniff detects only unlawful activity and does not implicate legitimate privacy interests).

We also find support in the decisions of federal appellate courts concluding that the use of a magnetometer (a metal detector) to scan for weapons at airports, courthouses, and other special locations is a reasonable search. *See, e.g., United States v. Albardo*, 495 F.2d 799, 803-06 (2d Cir. 1974) (airport); *United States v. Epperson*, 454 F.2d 769, 771-72 (4th Cir. 1972) (airport); *Klarfield v. United States*, 944 F.2d 583, 586 (9th Cir. 1991) (courthouse). In those contexts, the Government's interests are compelling, and the magnetometer's ability to detect not only weapons, but also keys, belt buckles, jewelry, and other harmless items does not otherwise render its use an unreasonable search. *See United States v. Bell*, 464 F.2d 667, 675 (2d Cir. 1972) (Friendly, J.); *Epperson*, 454 F.2d at 771-72. Regardless whether the Government's interests here are on par with preventing hijacking or airport and courthouse violence, EINSTEIN 2.0 technology promotes the Government's network-defense interests through a more limited and precise intrusion. The information provided to us indicates that EINSTEIN 2.0 technology is more precisely calibrated than a magnetometer to detect the materials (here, malicious computer codes) that pose a threat. *See supra* pp. 3-4. Hence, we believe that, like the use of the magnetometer in certain contexts, the use of EINSTEIN 2.0 technology to detect malicious computer code in Federal Systems Internet Traffic is a reasonable activity.

Furthermore, we understand that any information acquired or shared by DHS in the course of EINSTEIN 2.0 operations shall be subject to minimization procedures that are designed to minimize the acquisition, retention, and dissemination of non-publicly available information concerning United States persons. So, for example, even to the extent EINSTEIN 2.0 operations would acquire the content of malicious computer code that overlaps with human-readable text—e.g., the “I love you” virus from several years ago, or social engineering techniques that rely upon regular e-mail text to encourage the recipient to submit sensitive information, including personally identifiable information—we understand that these minimization procedures are intended to reduce further the impact of EINSTEIN 2.0 operations upon the privacy interests of United States persons in the content of their Internet communications. *Cf. In re Sealed Case*, 310 F.3d 717, 740 (FISA Ct. Rev. 2002) (noting importance of minimization procedures in holding that electronic surveillance pursuant to FISA was reasonable under the Fourth Amendment). In addition, we understand that DHS is required to develop auditing, oversight, and training procedures to ensure that its employees follow the procedures developed with respect to minimizing and protecting United States person information. We further understand that DHS is required to develop procedures for the development of signatures to be programmed into the EINSTEIN 2.0 sensors, to ensure that the sensors are limited only to the detection of malicious computer code. In light of these safeguards, we believe that EINSTEIN 2.0 operations will have a minimal impact upon the legitimate privacy rights of computer users.

We conclude that the important governmental interest in protecting Federal Systems from intrusion and exploitation at the hands of foreign intelligence services, transnational criminal enterprises, and rogue computer hackers, *see supra* p. 2, outweighs the limited impact on the privacy rights, if any, of computer users communicating through Federal Systems. *See Heckenkamp*, 482 F.3d at 1148 (there is a “compelling government interest” in maintaining “the

security of its network” and in determining the source of “unauthorized intrusion into sensitive files”); *Vernonia Sch.*, 515 U.S. at 661 (government must identify “an interest that appears *important enough* to justify the particular search at hand”). Based upon the information provided to us, we believe that EINSTEIN 2.0 operations would constitute a “reasonably effective means” of promoting those interests. *Earls*, 536 U.S. at 837 (activity must be “a reasonably effective means of addressing” government’s interest); *see Vernonia Sch.*, 515 U.S. at 663 (considering “the efficacy of [the] means for addressing the problem”). As explained *supra* pp. 4-5, EINSTEIN 2.0 operations are expected to improve the Government’s situational awareness regarding computer network intrusions and exploitations against Federal Systems and to strengthen the ability to defend Federal Systems across the entire Executive Branch. Because EINSTEIN 2.0 technology is designed to detect and to store only malicious computer code associated with previously signatures, they also “are reasonably related in scope” to the problem EINSTEIN 2.0 is intended to address—the use of known malicious computer code to conduct intrusions and exploitations against Federal Systems. *O’Connor*, 480 U.S. at 726 (plurality) (internal quotation marks omitted).

Therefore, even if EINSTEIN 2.0 operations did involve a “search” within the meaning of the Fourth Amendment, we conclude that those operations nonetheless would satisfy the reasonableness requirement of the Fourth Amendment. For that same reason, we also conclude that an Executive Branch employee’s agreement to the terms of the model log-on banner or the model computer-user agreement, or those of a banner or user agreement that are substantially equivalent to those models, constitutes valid, voluntary consent to the reasonable scope of EINSTEIN 2.0 operations, and, thus, does not impose any coercive unconstitutional condition upon federal employment.

III.

We now turn to the statutory issues. DOJ has advised that the deployment, testing, and use of EINSTEIN 2.0 technology would comply with the requirements of the Wiretap Act, FISA, the SCA, and the Pen/Trap Act where EINSTEIN 2.0 Participants obtain the consent of their employees through appropriate log-on banners or computer-user agreements. As we concluded with respect to the Fourth Amendment, we also conclude that EINSTEIN 2.0 operations would be consistent with the requirements of these statutes, provided that each EINSTEIN 2.0 Participant consistently adopts, implements, and enforces the model log-on banner or model computer-user agreement—or a log-on banner or computer-user agreement containing substantially equivalent terms establishing that the consent of its employees is “clearly given” and “clearly obtained.”

A.

We begin with the Wiretap Act. The Wiretap Act, as amended by title I of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (“ECPA”), and other subsequent statutes, prohibits the intentional “intercept[]” of any “electronic communication” unless authorized by law. 18 U.S.C. § 2511(1)(a) (2006); *see also id.* § 2511(1)(c) & (d) (prohibiting the intentional disclosure or use of the contents of electronic communications acquired in violation of section 2511(1)(a)). As relevant here, the Act defines

Opinions of the Office of Legal Counsel in Volume 33

“intercept” as the “acquisition of the contents of any . . . electronic . . . communication through the use of any electronic, mechanical, or other device.” *Id.* § 2510(4). EINSTEIN 2.0 technology would constitute a covered “device.” *See id.* § 2510(5) (defining “electronic, mechanical, or other devices” as any device “which can be used to intercept a[n] . . . electronic communication other than” certain specified devices not applicable here).

Because use of the EINSTEIN 2.0 sensors requires the creation of a full mirror copy of the Federal Systems Internet Traffic of EINSTEIN 2.0 Participants, we conclude that the operation of those sensors “acqui[re]s the contents” of an electronic communication within the meaning of the Act. The Wiretap Act defines “contents” to mean “any information concerning the substance, purport, or meaning” of a communication. 18 U.S.C. § 2510(8). And “electronic communication” is defined to mean “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, . . . electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce,” with certain exceptions not applicable here. *Id.* § 2510(12). The courts have held that communications that have not been recorded (to a medium such as a computer disk), viewed, or listened to have not been “acquired” within the meaning of the Wiretap Act. *See, e.g., United States v. Lewis*, 406 F.3d 11, 17-18 (1st Cir. 2004). Although the full mirror copy of Federal Systems Internet Traffic is only temporary, we believe the creation of the copy is sufficient to constitute an acquisition of the contents of communication under the Wiretap Act. Furthermore, even if creation of the temporary mirror copy were not sufficient to implicate the provisions of that Act, EINSTEIN 2.0 technology also acquires and stores, for later review by analysts, data packets from Federal Systems Internet Traffic containing malicious computer code associated with a signature. The acquisition and storage of these data packets, which are part of the “contents” of electronic communications, certainly constitutes an “intercept” within the meaning of the Wiretap Act. *See* 18 U.S.C. § 2510(4), (5), (8), & (12). Therefore, absent an exception, section 2511(1)(a) applies to at least some aspects of EINSTEIN 2.0 operations.

The Wiretap Act also prohibits a person or entity providing “electronic communication service” to “the public” from intentionally “divulg[ing] the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.” 18 U.S.C. § 2511(3)(a). It is unclear whether the federal Government provides “electronic communication service” to “the public.” It reasonably could be argued that an EINSTEIN 2.0 Participant does offer Web sites and other Internet-related services that enable the transmission of electronic communications to and from the public, qualifies as a provider of electronic communication service to the public. *See id.* § 2510(15) (defining “electronic communication service” as “any service which provides to users thereof the ability to send or receive wire or electronic communication service”); *Black’s Law Dictionary* 1227 (6th ed. 1990) (defining public as “aggregate of the citizens”; “everybody”; “the community at large”). We need not decide the issue today, for even if the Government is a provider of electronic communication service to the public, we do not believe that EINSTEIN 2.0 operations run afoul of the prohibitions in the Wiretap Act on the divulging of the contents of wire and electronic communications.

We conclude that EINSTEIN 2.0 operations do not constitute an *unlawful* interception or divulging of the contents of Internet communications under the Wiretap Act for two reasons. First, where EINSTEIN 2.0 Participants obtain the consent of their employees through appropriate log-on banners or computer-user agreements, there would be no violation of the Wiretap Act. Second, there is a strong argument that the Government's EINSTEIN 2.0 operations are subject to the "rights or property" exception to the Wiretap Act. We also discuss, but do not decide, whether EINSTEIN 2.0 operations fall within the new "computer trespasser" exception to the prohibitions of the Wiretap Act.

1.

Under the Act, "[i]t shall not be unlawful . . . for a person acting under color of law to intercept a[n] . . . electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception." 18 U.S.C. § 2511(2)(c). Likewise, a person providing electronic communication service to the public "may divulge the contents of any such communication" either "to a person . . . authorized, or whose facilities are used, to forward such communications to its destination," *id.* § 2511(3)(b)(iii), or "with the lawful consent of the originator or any addressee or intended recipient of such communication," *id.* § 2511(3)(b)(ii). These exceptions take EINSTEIN 2.0 operations, if conducted consistent with the terms of the EINSTEIN 2.0 MOA, outside the scope of the prohibitions in the Wiretap Act.

The exception in section 2511(2)(c) applies to the interception of the contents of an Internet communication where an executive department or agency is a direct party to the communication, such as where an individual files a form with an agency through a Web site or responds online to a government survey. There is no violation of the Wiretap Act where "a person acting under color of law" intercepts an electronic communication provided that "one of the parties to the communication has given prior consent to such interception." 18 U.S.C. § 2511(2)(c). For purposes of section 2511(2)(c), DHS is "a person acting under color of law" in the course of conducting EINSTEIN 2.0 operations. *Id.* § 2510(6) (defining person to include any "agent" of the United States Government). *See Nardone v. United States*, 302 U.S. 379, 384 (1937) (government bound by wiretap laws because "the sovereign is embraced by general words of a statute intended to prevent injury"); *cf.* 18 U.S.C. § 2520(a) (2006) (plaintiff may recover civil damages from "a person or entity, other than the United States," which engaged in that violation). By entering into an MOA with DHS, an EINSTEIN 2.0 Participant has signaled its consent to the interception by EINSTEIN 2.0 sensors and DHS of the content of Internet communications to which it is a party. Therefore, DHS lawfully may intercept the contents of an EINSTEIN 2.0 Participant's Internet communications with individuals under the Wiretap Act. *Id.* § 2511(2)(c). For the same reason, it also is lawful for an EINSTEIN 2.0 Participant to divulge the contents of an Internet communication to DHS for the purposes of EINSTEIN 2.0 operations where an EINSTEIN 2.0 Participant is one of the addressees or recipients of the communication. *Id.* § 2511(3)(b)(ii) (person may divulge contents of communication "with the lawful consent of the originator or any addressee or intended recipient of such communication").

With respect to intercepting and divulging the contents of Internet communications involving Executive Branch employees and individuals outside the Executive Branch, we do not

Opinions of the Office of Legal Counsel in Volume 33

believe that such actions would violate the prohibitions in the Wiretap Act. To begin with, EINSTEIN 2.0 operations do not unlawfully “divulge” the contents of Internet communications with Executive Branch employees, because the federal Government is “authorized,” and its “facilities are used, to forward such communications to [their] destination.” 18 U.S.C. § 2511(3)(b)(iii). Internet communications cannot get to or from Executive Branch employees at work without routing through the facilities of Federal Systems.

There also is no violation of either the interception or the divulging prohibitions of the Wiretap Act where one of the parties to a communication has given consent. *See* 18 U.S.C. § 2511(2)(c) (“prior consent” required for intercept); *id.* § 2511(3)(b)(ii) (“lawful consent” required for divulging). An EINSTEIN 2.0 Participant cannot consent to the interception of the contents of the communications of its employees on their behalf; rather, the consent of the employee who is the sender or the recipient of the communication is required. *See Television Surveillance Opinion*, 3 Op. O.L.C. at 67 (consent to surveillance is “not predicated on the consent of the owner of the pertinent property, but rather on the consent of the person to whom the targeted individual reveals his communications or activities”); *see also Caceres*, 440 U.S. at 750 (“[F]ederal statutes impose no restrictions on recording a conversation with the consent of one of the conversants.”); *United States v. Barone*, 913 F.2d 46, 49 (2d Cir. 1990) (one-party consent obviates the need to obtain a court order under the Wiretap Act). As with any other person, an employee’s consent under the Wiretap Act also must be provided voluntarily. *See United States v. Hernandez*, 93 F.3d 1493, 1500 (10th Cir. 1996). Here, an employee’s valid, voluntary consent is expressly apparent from his clicking through the log-on banner or signing the computer-user agreement in order to access a Government-owned information system. *See supra* pp. 16-21; Memorandum for Ronald D. Lee, Associate Deputy Attorney General, from William Treanor, Deputy Assistant Attorney General, Office of Legal Counsel, *Re: Report of the Working Group on Access to Government Property (Second Draft)* at 5 (June 1, 2000) (consent exception in Wiretap Act satisfied where employee clicks through log-on banner acknowledging monitoring of electronic communications in order to access DOJ’s computer network).

An Executive Branch employee’s consent to interception or divulging of the contents of his Internet communications also may be implied where the “circumstances indicat[e] that the [individual] knowingly agreed to the surveillance.” *United States v. Van Poyck*, 77 F.3d 285, 292 (9th Cir. 1996) (quoting *United States v. Amen*, 831 F.2d 373, 378 (2d Cir. 1987) (federal inmate consented to interception of phone calls where notice that inmate calls were monitored was ubiquitous)). Under the Wiretap Act, “as in other settings, consent inheres where a person’s behavior manifests acquiescence or a comparable voluntary diminution of his or her otherwise protected rights.” *Griggs-Ryan v. Smith*, 904 F.2d 112, 116 (1st Cir. 1990) (tenant consented to landlord’s recording of phone calls where tenant knew that all calls were being recorded); *accord United States v. Staves*, 383 F.3d 977, 981 (9th Cir. 2004) (party to communication impliedly consents to monitoring where circumstances “indicate that [he] knew that interception was likely and agreed to the monitoring”). Where “language or acts . . . tend to prove (or disprove) that a party knows of, or assents to, encroachments” on a routine expectation of privacy, that party has manifested his consent for purposes of the Wiretap Act. *Griggs-Ryan*, 904 F.2d at 117; *see Van Poyck*, 77 F.3d at 292 (similar).

Here, no Executive Branch employee who has read the model log-on banner or computer-user agreement (or a log-on banner or computer-user agreement with substantially equivalent terms) and who nonetheless has logged on to a Government-owned information system could reasonably claim not to have knowledge that monitoring, interception, and searches of his Internet communications would occur. The employee's use of Government-owned information systems despite that knowledge would establish voluntary consent to any such monitoring, interception, or search. *See supra* pp. 13, 16-21.¹⁰ Therefore, we believe that EINSTEIN 2.0 operations would comply with the Wiretap Act as long as EINSTEIN 2.0 Participants consistently adopt, implement, and enforce the terms of appropriate log-on banners or computer-user agreements, as discussed in this memorandum.

2.

Even absent the consent of Executive Branch employees, there is a reasonable basis to conclude that the use of EINSTEIN 2.0 technology to protect Federal Systems comes within the express terms of the "rights or property" exception to the prohibitions in the Wiretap Act, 18 U.S.C. § 2511(2)(a)(i). The "rights or property" exception provides in relevant part that the prohibitions in the Act shall not apply to the "intercept, disclosure, or use" of an "electronic communication" by a "provider of a wire or electronic communication service . . . engaged in any activity which is a necessary incident to . . . the protection of the rights or property of the provider of that service." *Id.*

We believe that this provision may be applied to the Government here as a "provider" of "electronic communication service[s]" for its employees. Executive Branch departments and agencies provide the necessary computers, network infrastructure, facilities, and connectivity to the Internet that enable Executive Branch employees "to send or receive" electronic communications. 18 U.S.C. § 2510(15) (defining "electronic communication service"). The courts have held that to benefit from the rights or property exception, the electronic communication service provider's activities must protect the provider's own rights or property, and not those of any third party, such as a customer. *See, e.g., Campiti v. Walonis*, 611 F.2d 387, 393 (1st Cir. 1979) (rights or property exception does not apply to a person who is not an agent of the telephone company for monitoring that "had nothing to do with telephone company equipment or rights"); *United States v. Auler*, 539 F.2d 642, 645-46 (7th Cir. 1976) (telephone companies intercepting communications under section 2511(2)(a)(i) may share those communications with the government only to the extent necessary to protect telephone company's rights or property). EINSTEIN 2.0 technology is owned, operated, and controlled by DHS, and we understand that it is to be used solely for the protection of the Government's rights and property in Federal Systems. *See supra* p. 3.

¹⁰ Similarly, no reasonable person communicating directly with an agency of the federal Government through the Internet, such as by filing a form on an agency Web site, could claim not to know that his communication would be acquired by the Government. Indeed, that is the entire purpose of communicating with the Government. *See supra* p. 14. Hence, the individual impliedly would consent to the Government's interception of the contents of his communication. *See Caller ID Opinion*, 20 Op. O.L.C. at 320 & n.13 (dialing 911 constitutes implicit consent to Government's direct monitoring of an emergency call).

Opinions of the Office of Legal Counsel in Volume 33

The legislative history of the rights or property exception in the Wiretap Act arguably speaks only to the efforts of telephone companies to monitor calls in order to prevent callers from using “blue boxes” to avoid paying for long-distance telephone calls. See S. Rep. No. 90-1097, at 67 (1967), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2182. Nevertheless, we believe that “the plain meaning of Congress’[s] language” in the “rights or property” exception includes EINSTEIN 2.0 operations “within its ambit.” *United States v. Savage*, 564 F.2d 728, 731 (5th Cir. 1977). The courts have construed the “necessary” language in the Wiretap Act provision “to impose a standard of reasonableness upon” the provider’s activities to protect his rights or property. *United States v. Harvey*, 540 F.2d 1345, 1351 (8th Cir. 1976); see, e.g., *United States v. McLaren*, 957 F. Supp. 215, 220 (M.D. Fla. 1997) (similar). As in the Fourth Amendment context, reasonableness is “assessed under the facts of each case.” *Harvey*, 540 F.2d at 1352 n.9. The “rights or property” exception does not strictly *require* “minimization” of the acquisition of communication contents by a provider, *McLaren*, 957 F. Supp. at 220, but a provider’s activities are reasonable under the exception where they involve only “minimal interception” of communications. *Harvey*, 540 F.2d at 1351.

We believe that the Government’s use of EINSTEIN 2.0 technology to detect intrusions and exploitations against Federal Systems is reasonably necessary to protect the federal Government’s rights with respect to its exclusive use of Federal Systems and its property interests in the integrity and security of its networks and data. For the reasons we have noted already, see *supra* pp. 18-21, we believe that EINSTEIN 2.0 operations would involve the minimal acquisition and storage of communications necessary to detect malicious network activity directed against Federal Systems. EINSTEIN 2.0 operations are limited to the detection and storing of data packets containing only malicious computer code associated with computer intrusions and exploitations, and are reasonably designed to protect Federal Systems without acquiring any additional content of Internet communications that is unrelated to that goal. Thus, EINSTEIN 2.0 operations are appropriately limited in scope to what is reasonably necessary to protect governmental rights and property against computer intrusions and exploitations. See *Harvey*, 540 F.2d at 1351 (recording of limited portion of phone calls to identify use of technology to evade paying for long-distance calls is “reasonable”); *United States v. Freeman*, 524 F.2d 337, 341 (7th Cir. 1975) (taping of conversations for no more than two minutes and only when blue box was in use was “necessary and in line with the minimal invasion of privacy contemplated by the statute”); cf. *Auler*, 539 F.2d at 646 (monitoring and recording of all calls, regardless whether made using a blue box, acquired “far more information” than the telephone company “needed to protect its interests”); *McLaren*, 957 F. Supp. at 220 (interception, recording, and disclosure of complete phone calls “having nothing whatever to do” with abuse of telephone company’s service is unreasonable because those actions “could not possibly be ‘necessary’” to protecting the company’s rights).

Therefore, even absent employee consent, there is a strong basis in the text of the “rights or property” exception to the Wiretap Act to believe that the Government’s activities under EINSTEIN 2.0 would not violate the prohibitions in the Wiretap Act. That being said, however, there are very few cases applying the rights or property exception since the mid-1970s, and almost none involving computer networks, the Internet, or defenses against cyber intrusions and exploitations, and none involving the Government in protecting its own rights or property, as opposed to a private communications provider protecting its private property. Accordingly, we

believe there is some uncertainty regarding how the courts would view a defense of EINSTEIN 2.0 operations based upon the “rights or property” exception to the Wiretap Act.

3.

Finally, we discuss briefly the “computer trespasser” exception in the Wiretap Act, 18 U.S.C. § 2511(2)(i), which was added to the Wiretap Act by section 217 of the USA PATRIOT Act, *see* Public Law No. 107-56, 115 Stat. 272, 291 (2001). Section 2511(2)(i) permits “a person acting under color of law” to “intercept” the contents of “wire or electronic communications of a computer trespasser transmitted to, through, or from [a] protected computer” on four conditions: First, “the owner or operator of the protected computer authorizes the interception of the computer trespasser’s communications on the protected computer.” Second, “the person acting under color of law is lawfully engaged in an investigation.” Third, “the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser’s communications will be relevant to the investigation.” And fourth, “such interception does not acquire communications other than those transmitted to or from the computer trespasser.” 18 U.S.C. § 2511(2)(i)(I)-(IV). The phrase “protected computer” has the same definition as in 18 U.S.C. § 1030(e)(2), *see id.* § 2510(20) (defining “protected computer”), which includes the Government-issued computers of EINSTEIN 2.0 Participants at issue here. “Computer trespasser” is defined to mean “a person who accesses a protected computer without authorization” and “does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.” *Id.* § 2510(21)(A) & (B).

We need not discuss the first three requirements of the computer trespasser exception. Even assuming that EINSTEIN 2.0 operations satisfy these requirements, it is questionable that EINSTEIN 2.0 operations satisfy the final requirement. The computer trespasser exception is applicable only if interception of the contents of communications “does not acquire communications other than those transmitted to or from the computer trespasser.” 18 U.S.C. § 2511(2)(i)(IV). We understand that EINSTEIN 2.0 technology is designed to detect and to store only packets containing malicious computer code associated with a signature. Accordingly, it could be argued that it would not acquire communications other than the malicious code sent over the Internet by computer trespassers, as defined in section 2510(21). However, EINSTEIN 2.0 technology also can acquire the contents of communications to or from persons who do not satisfy the definition of “computer trespasser.” To take just one example, an Executive Branch employee—even one who intentionally includes malicious computer code in his Internet communications at work—does not appear to be a “computer trespasser” within the scope of the definition. *See id.* § 2510(21)(B) (defining “computer trespasser” to exclude a “person known by the owner or operator of the protected computer to have an existing contractual relationship . . . for access to all or part of the protected computer”).¹¹ EINSTEIN 2.0 operations, however, nonetheless would acquire the contents of their communications.

¹¹ That does not mean that the Government would be prohibited from acquiring the communications of an employee or contractor who intentionally incorporates malicious code in their Internet communications. Rather, some other statutory exception—such as consent or the rights or property exception—may authorize that result.

Opinions of the Office of Legal Counsel in Volume 33

We do not decide, however, whether the computer trespasser exception would or would not apply to EINSTEIN 2.0 operations. In light of the other legal justifications for EINSTEIN 2.0 operations under the Wiretap Act, we need not rely upon this provision.

B.

We next consider whether the provisions in title I of FISA, which govern the conduct of “electronic surveillance” within the United States, and in revised title VII of FISA, which govern, among other things, the acquisition of foreign intelligence information from United States persons outside the United States, apply to the deployment, testing, and use of EINSTEIN 2.0 technology. We conclude that they do not, provided that EINSTEIN 2.0 Participants obtain the consent of their employees through the terms of log-on banners or computer-user agreements, as discussed throughout this memorandum.

1.

Under 50 U.S.C.A. § 1809(a)(1) (West 2008), it is a felony for a person acting “under color of law” to engage intentionally in “electronic surveillance” as defined in title I of FISA, *see* 50 U.S.C. § 1801(f), “except as authorized” by FISA, the Wiretap Act, the SCA, the Pen/Trap Act, or any other “express statutory authorization that is an additional exclusive means for conducting electronic surveillance” under 50 U.S.C.A. § 1812(b) (West 2008). *See also id.* § 1810 (West 2008) (establishing civil penalties for violations of section 1809(a)(1)). As we have established in Part III.A., EINSTEIN 2.0 operations would not be prohibited by the Wiretap Act. Thus, it could be argued that they are “authorized” under the Wiretap Act. On this view, FISA does not govern activity that is expressly permitted under provisions in the Wiretap Act, such as activity falling within the terms of the consent or the rights or property exception. *Cf. Freeman*, 524 F.2d at 340 & n.5 (phrase “[e]xcept as authorized by [the Wiretap Act]” in 47 U.S.C. § 605(a) (1970) “permits” telephone companies to protect their rights or property under section 2511(2)(a)(i) notwithstanding any otherwise applicable terms of section 605(a)). Accordingly, EINSTEIN 2.0 operations permitted under the rights or property exception of the Wiretap Act would be authorized notwithstanding the electronic surveillance provisions of FISA (and notwithstanding the absence of a rights or property exception in FISA).

There is much to recommend that view, although the better reading of “authorized” may be that the term refers to orders obtained under the procedures of the Wiretap Act, the SCA, the Pen/Trap Act, or another covered statute, rather than to activities that merely are not prohibited by those statutes. *Cf. United States v. Keen*, 508 F.2d 986, 988 (9th Cir. 1974) (“Section 2511(2)(c) is worded as an exception to [the] general prohibition of judicially non-authorized wire taps, not as a positive authorization of such taps.”). We need not and do not resolve this issue today. Rather, we assume for the purposes of this memorandum that title I of FISA applies to the deployment, testing, and use of EINSTEIN 2.0 technology if those actions constitute “electronic surveillance” within the meaning of 50 U.S.C. § 1801(f).

Section 1801(f) sets forth four separate definitions of “electronic surveillance.” They are as follows:

(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communications sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18;

(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, 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 within the United States; or

(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

50 U.S.C. § 1801(f)(1)-(4). EINSTEIN 2.0 operations that scan, acquire, and store copies of data packets containing malicious computer code from Federal Systems Internet Traffic constitute an “acquisition” of the “contents” of a communication. *Id.* § 1801(n) (defining “contents” to include “any information concerning the identity of the parties to . . . communications or the existence, substance, purport, or meaning of that communication”).

Nevertheless, paragraphs (1) and (3) of section 1801(f) do not apply to EINSTEIN 2.0 operations. Those operations do not constitute electronic surveillance under section 1801(f)(1), because EINSTEIN 2.0 sensors generally would not target any “particular, known United States person” in the United States. Nor do EINSTEIN 2.0 operations constitute electronic surveillance within the meaning of section 1801(f)(3), because the EINSTEIN 2.0 sensors do not acquire the contents of any “radio communication.” As explained *supra* in Part I, EINSTEIN 2.0 sensors are to scan only a mirror copy of Federal Systems Internet Traffic created as that traffic passes through the facilities located at the Government’s TICs. Furthermore, even if section 1801(f)(1) and section 1801(f)(3) did apply to EINSTEIN 2.0 operations, the use of EINSTEIN 2.0 technology still does not constitute “electronic surveillance” under those definitions, because the use of those sensors does not implicate “a person’s reasonable expectation of privacy.” See *supra* pp. 7-14 and *infra* p. 30.

That leaves section 1801(f)(2) and (4). Section 1801(f)(2) applies to EINSTEIN 2.0 operations only if EINSTEIN 2.0 technology acquires the contents of “wire communication[s],”

Opinions of the Office of Legal Counsel in Volume 33

which FISA defines as “any communication while it is being carried by a wire, cable, or other like connection furnished or operated by . . . a common carrier . . . providing or operating such facilities for the transmission of interstate or foreign communications.” 50 U.S.C. § 1801(i); see H.R. Rep. No. 95-1283, at 66-67 (1978) (communications are wire communications “only when they are carried by a wire furnished or operated by a common carrier”). FISA does not define the term “common carrier.” We need not decide whether EINSTEIN 2.0 operations acquire the contents of communications while being carried by the wire facilities of a common carrier. Even if they do, the use of EINSTEIN 2.0 technology does constitute electronic surveillance under section 1801(f)(2) as long as the Government obtains “the consent of any party” to a communication to acquire the contents of that communication. 50 U.S.C. § 1801(f)(2).

Because the consent exception in section 1801(f)(2) concerns the same subject matter—consent of a party to a communication—as section 2511(2)(c), we construe the two provisions *in pari materia*. See *Wachovia Bank, N.A. v. Schmidt*, 126 S. Ct. 941, 950 (2006) (statutes addressing a similar subject matter should be read “as if they were one law”) (internal quotation marks omitted); *Authority of USDA to Award Monetary Relief for Discrimination*, 18 Op. O.L.C. 52, 69 (1994) (“Statutes addressing the same subject matter—that is, statutes ‘*in pari materia*’—should be construed together.”). That construction is consistent with the stated views of the Senate Select Committee on Intelligence and the Senate Committee on the Judiciary in their respective committee reports on the legislation that ultimately would become FISA. See S. Rep. No. 95-604, pt. I, at 35 (1978) (definition of electronic surveillance “has an explicit exception where any party has consented to the interception. This is intended to perpetuate the existing law regarding consensual interceptions found in 18 U.S.C. § 2511(2)(c).”), reprinted in 1978 U.S.C.C.A.N. 3904, 3936-37; S. Rep. No. 95-701, at 37 (1978) (same), reprinted in 1978 U.S.C.C.A.N. 3973, 4006. Accordingly, for the same reasons already noted above with respect to the Wiretap Act, we believe that the Government could obtain valid consent under section 1801(f)(2) through consistent and actual use of log-on banners or computer-user agreements. See *United States v. Missick*, 875 F.2d 1294, 1299 (7th Cir. 1989) (section 1801(f)(2) does not apply to acquisition of content of telephone calls where one of the parties consented).

For that same reason, we do not believe that EINSTEIN 2.0 operations constitute “electronic surveillance” under section 1801(f)(4). It is plain that the use of EINSTEIN 2.0 technology constitutes “the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information.” 50 U.S.C. § 1801(f)(4). But regardless whether that technology would acquire the contents of communications “other than from” the wire facilities of a common carrier, EINSTEIN 2.0 operations would not fall within the scope of section 1801(f)(4). As long as EINSTEIN 2.0 Participants consistently adopt, implement, and enforce the use of appropriate log-on banners or computer-user agreements as discussed in this memorandum, EINSTEIN 2.0 technology would not acquire the contents of Internet communications under circumstances where there is a “reasonable expectation of privacy” and a warrant “would be required for law enforcement purposes.” See *supra* pp. 7-14, 23-25; see also *Interception of Radio Communication*, 3 Op. O.L.C. 240, 241 (1979) (phrase “reasonable expectation of privacy” in FISA incorporates “the standard of constitutionally protected privacy interests”); H.R. Rep. No. 95-1283, pt. 1, at 53 (1978) (under section 1801(f)(4) “the acquisition of information [must] be under circumstances in which a person has a constitutionally protected right of privacy. There may be no such right in those situations where

the acquisition is consented to by at least one party to the communication”); S. Rep. No. 95-701, at 37 (1978) (same).

Therefore, EINSTEIN 2.0 operations would not constitute “electronic surveillance” under title I of FISA as long as EINSTEIN 2.0 Participants consistently adopt, implement, and enforce the terms of appropriate log-on banners or computer-user agreements, as discussed in this memorandum.

2.

For the same reasons, we do not believe that the use of EINSTEIN 2.0 technology with respect to the Federal Systems Internet Traffic of Executive Branch employees outside the United States, such as (hypothetically) employees of the Department of State or the Central Intelligence Agency, implicates revised title VII of FISA. As applicable here, section 703(a)(1) of FISA provides that the Foreign Intelligence Surveillance Court (“FISC”) shall have jurisdiction over the “the targeting of a United States person reasonably believed to be located outside the United States to acquire foreign intelligence information if the acquisition constitutes electronic surveillance” under FISA. 50 U.S.C.A. § 1881b(a)(1) (West 2008). And section 704(a)(2) of FISA generally prohibits elements of the Intelligence Community from “intentionally target[ing], for the purpose of acquiring foreign intelligence information, a United States person reasonably believed to be located outside the United States in circumstances where [the person] has a reasonable expectation of privacy and where a warrant would be required if the acquisition were conducted inside the United States for law enforcement purposes.” *Id.* § 1881c(a)(2).

We have no reason to believe that EINSTEIN 2.0 operations generally would involve the intentional targeting of any United States person employed by an EINSTEIN 2.0 Participant outside the United States in order to acquire “foreign intelligence information” as defined in 50 U.S.C. § 1801(e). Even assuming for the sake of argument that EINSTEIN 2.0 operations would satisfy those requirements, we do not believe those operations would satisfy the other jurisdictional requirements in sections 1881b(a)(1) or 1881c(a)(2), provided that EINSTEIN 2.0 Participants employing United States persons outside the United States consistently adopt, implement, and enforce appropriate notice and consent procedures, as discussed in this memorandum. In that circumstance, there would be no “electronic surveillance” as defined in section 1801(f)(1)-(4), and, thus, section 1881b(a)(1) would be inapplicable. *See supra* pp. 28-31. Likewise, there would be no reasonable expectation of privacy and a warrant would not be required for law enforcement purposes for either of two reasons: there would be no search under the Fourth Amendment, *see supra* pp. 7-14, or there would be proper consent, thus obviating the need for a warrant and probable cause, *see supra* pp. 13, 16-21. Under either rationale (or both), the prohibition in section 1881c(a)(2) would not apply. Therefore, we do not believe that EINSTEIN 2.0 operations would be subject to revised title VII of FISA.

C.

We also conclude that the relevant provisions of the Stored Communications Act would not apply to EINSTEIN 2.0 operations, provided that EINSTEIN 2.0 Participants consistently

Opinions of the Office of Legal Counsel in Volume 33

adopt, implement, and enforce the terms of appropriate log-on banners or computer-user agreements, as discussed in this memorandum. As relevant here, the SCA prohibits a person or entity “providing an electronic communication service to the public” from knowingly “divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service.” 18 U.S.C. § 2702(a)(1) (2006). As already noted with respect to the Wiretap Act, it is unclear that the federal Government—which does offer Web sites and other Internet-related services that enable the transmission of electronic communications to and from the public—qualifies as a provider of electronic communication service to the public under the SCA. *See supra* p. 22. The matter is far from settled. *Compare Andersen Consulting LLP v. UOP*, 991 F. Supp. 1041, 1042-43 (N.D. Ill. 1998) (computer system of partnership used to communicate with third parties does not provide electronic communication service to the public within the meaning of the SCA), *with Bohach v. City of Reno*, 932 F. Supp. 1232, 1236 (D. Nev. 1996) (City of Reno is an “electronic communication service provider” under the SCA because it provides the terminals, computers, pages, and software that enables its own personnel to send and to receive electronic communications). We need not decide the issue, for even if the Government is a provider of electronic communication service to the public, we do not believe that EINSTEIN 2.0 operations would run afoul of the SCA.

EINSTEIN 2.0 operations would implicate the prohibition in section 2702(a)(1) if the temporary mirroring of all Federal Systems Internet Traffic of EINSTEIN 2.0 Participants divulges the content of an electronic communication “while in electronic storage.” The SCA defines “electronic storage” to mean:

- (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
- (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

Id. § 2510(17)(A) & (B). The courts have interpreted section 2510(17)(A) to apply only to an electronic communication stored temporarily on a provider’s server pending delivery of the communication to the recipient. *See, e.g., In re DoubleClick, Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 511-12 (S.D.N.Y. 2001). As noted in Part I, *supra* p. 4, EINSTEIN 2.0 technology does not have any effect upon the transmission of wire or electronic communications to their intended recipients. Rather, EINSTEIN 2.0 operations will make a mirror copy of every packet in Federal Systems Internet Traffic and will scan that copy to detect known signatures. This copy is “temporary” storage of communications “incidental” to their transmission, in the sense that the storage is related to the transmission of those communications. But arguably it is not “intermediate” in the process of that transmission, because the temporary copy is not created as part of a step in the chain of transmitting the communication to its intended recipient. Rather, the copy is made for the separate purpose of enabling EINSTEIN 2.0 sensors to detect malicious computer code embedded in Federal Systems Internet Traffic. Indeed, the EINSTEIN 2.0 scanning process occurs out-of-line from the transmission process, even if it is related to the in-line transmission of Federal Systems Internet Traffic.

Nor do we understand that EINSTEIN 2.0 operations would divulge the content of any communication while in storage “for purposes of backup protection” within the meaning of section 2510(17)(B), even under a broader reading of “backup protection” than DOJ has embraced in litigating the scope of that provision. *See Theofel v. Farey Jones*, 341 F.3d 978, 985 (9th Cir. 2003) (backup protection means “storing a message on a service provider’s server after delivery to provide a second copy of the message in the event that the user needs to download it again”). Because the EINSTEIN 2.0 sensors scan a mirror copy of Federal Systems Internet Traffic for the purpose of detecting malicious computer code, there is no routing of the contents of any communication stored by an ISP for purposes of backup protection. It is true that EINSTEIN 2.0 technology would store data packets containing malicious computer code for later review by DHS analysts. But the “purpose” of any storage and subsequent review by analysts of blocked data packets would be to prevent intrusions and exploitations against Federal Systems, and not “to provide a second copy of the message in the event that the user needs to download it again.” *Id.* at 985. Therefore, we have no reason to believe that EINSTEIN 2.0 operations would divulge the contents of communications stored for backup protection.

Even if section 2702(a)(1) would apply to EINSTEIN 2.0 operations, scanning Federal Systems Internet Traffic for malicious computer code would fall within the SCA’s consent exception in 18 U.S.C. § 2702(b)(3) as long as EINSTEIN 2.0 Participants consistently adopt, implement, and enforce the terms of appropriate log-on banners or computer-user agreements, as discussed in this memorandum. Section 2702(b)(3) states in relevant part that an electronic communication service provider “may divulge the contents of a communication . . . with the lawful consent of the originator or an addressee or intended recipient of such communication.” *Id.*; *see also id.* § 2702(c)(2) (provider may divulge information pertaining to subscriber or customer of electronic communication service, but not the contents of that communication, “with the lawful consent of the customer or subscriber”). We have interpreted a similar consent exception in 18 U.S.C. § 2703(c)(1)(B)(iii) (2006), which states that a provider shall divulge a record pertaining to the identity of a subscriber or customer—but not the contents of a communication—to a governmental entity that “has the consent” of the customer or subscriber, *in pari materia* with the consent exception in the Wiretap Act. *See Caller ID Opinion*, 20 Op. O.L.C. at 319 & n.12 (interpreting consent exception in section 2703(c)(1)(B)(iii) in accord with the consent exception in the Wiretap Act). We also construe the consent exception in section 2702(b)(3)—which is even more closely analogous to the consent exception in section 2511(2)(c) than is section 2703(c)(1)(B)(iii)—*in pari materia* with section 2511(2)(c). *See supra* p. 30. For the reasons already noted with respect to the consent exception in the Wiretap Act, *see supra* pp. 23-25, to the extent the SCA applies to EINSTEIN 2.0 operations, we believe that the Government could obtain proper consent under section 2702(b)(3) and (c)(2) through the consistent and actual use of log-on banners or computer-user agreements.¹²

¹² EINSTEIN 2.0 operations also may fall within the “rights or property” exceptions to the SCA, *see* 18 U.S.C. § 2702(b)(5), (c)(3). The SCA’s “rights or property” exceptions are substantively similar to the parallel exception in the Wiretap Act. The SCA’s first rights or property provision states that a provider of electronic communication service to the public may divulge the contents of a stored communication “as may be necessarily incident . . . to the protection of the rights or property of the provider of that service.” 18 U.S.C. § 2702(b)(5). Another provision in the SCA permits a provider of electronic communication service to the public to disclose non-content information regarding a subscriber or a customer “as may be necessarily incident to . . . the protection of the rights or property of the provider of that service.” *Id.* § 2702(c)(3). In light of the similarities in wording and

*Opinions of the Office of Legal Counsel in Volume 33***D.**

Finally, we conclude that the Pen/Trap Act would not apply to EINSTEIN 2.0 operations where EINSTEIN 2.0 Participants consistently adopt, implement, and enforce the terms of appropriate log-on banners or computer-user agreements, as discussed in this memorandum. Section 3121(a) of title 18, United States Code, provides that “[e]xcept as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or” FISA. 18 U.S.C. § 3121(a) (2006). As relevant here, the statute defines a “pen register” as a “device . . . which records or decodes . . . routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication.” *Id.* § 3127(3) (2006). And a “trap and trace device” means “a device . . . which captures the incoming electronic or other impulses which identify . . . routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.” *Id.* § 3127(4).¹³

We assume for the purposes of this memorandum that the use of EINSTEIN 2.0 technology would fall within the definitions of both a pen register and a trap and trace device, because they can both “record” and “capture,” 18 U.S.C. § 3127(3) and (4), information that identifies routing, addressing, and signaling information for data packets that are part of Federal Systems Internet Traffic. *See supra* pp. 3-4, 7. Hence, absent an exception, we assume that the Government would be required to obtain a court order before the deployment, testing, and use of EINSTEIN 2.0 technology. *See* 18 U.S.C. § 3123 (2006).

As with the Wiretap Act, FISA, and the SCA, obtaining the valid consent of Executive Branch employees also exempts EINSTEIN 2.0 operations from any applicable requirement of the Pen/Trap Act. Section 3121(a) “does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service . . . where the

subject matter between the SCA’s rights or property exceptions and the Wiretap Act’s parallel provision, we construe them *in pari materia*. *See supra* pp. 30 & 33.

A crucial difference, however, between the “rights or property” exceptions in the SCA and the one in the Wiretap Act is that the SCA provisions apply only to a provider of electronic communication service *to the public*, whereas the Wiretap Act provision applies to *any* provider of such service, whether to the public or otherwise. As we noted, it is debatable whether the Government is a “provider” of electronic communication service to the public under the SCA. *See supra* pp. 22 & 32. Assuming that the Government is a public provider of electronic communication service, the SCA’s rights or property exceptions apply to any action under EINSTEIN 2.0 divulging the contents of stored electronic communications or non-content information concerning a subscriber or a customer that is reasonably necessary to protect Federal Systems. *See supra* pp. 25-27. Of course, if the Government is not a public provider, then the provisions of the SCA do not apply to it in any event.

¹³ Title III of FISA also establishes a statutory basis for the Government to obtain an authorization from the FISC to install a pen register or a trap and trace device in order to acquire certain foreign intelligence information. *See* 50 U.S.C. §§ 1841-1846 (2000 & Supp. V 2005). Under FISA, the terms “pen register” and “trap and trace device” have the same meanings as used in 18 U.S.C. § 3127(3) and (4). *See* 50 U.S.C. § 1841(2).

consent of the user of that service has been obtained.” 18 U.S.C. § 3121(b)(3).¹⁴ We believe that an EINSTEIN 2.0 Participant providing Internet service to its employees through Government-owned information systems and its Federal Systems would qualify as a “provider of electronic . . . communication service” within the meaning of the Pen/Trap Act. *See supra* pp. 25; 18 U.S.C. § 2510(15). Accordingly, the Government would be exempt from the prohibitions of the Pen/Trap Act with respect to EINSTEIN 2.0 operations where the “consent” of the “user[s]” of their electronic communication service “has been obtained.” With respect to both entities, we believe that the “user” whose consent needs to be obtained is the Executive Branch employee using a Government-owned computer at an IP address that is subject to EINSTEIN 2.0 operations. For the same reasons discussed above we believe that EINSTEIN 2.0 Participants could obtain proper consent from their employees under section 3121(b)(3) through the consistent adoption, implementation, and enforcement of appropriate log-on banners or computer-user agreements, as discussed in this memorandum. Therefore, we conclude that the deployment, testing, and use of EINSTEIN 2.0 technology would not constitute the unauthorized installation or use of a pen register or a trap and trace device under 18 U.S.C. § 3121(a).¹⁵

/s/

STEVEN G. BRADBURY
Principal Deputy Assistant Attorney General

¹⁴ The consent exception in section 3121(b)(3) also applies to the provisions in FISA authorizing the installation or use of such devices to acquire foreign intelligence information.

¹⁵ EINSTEIN 2.0 operations also may fall within the “rights or property” exception to the Pen/Trap Act. Section 3121(b)(1) provides that the prohibitions of that Act do not apply with respect to the use of such technology “by a provider of electronic or wire communication service . . . relating to . . . the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service.” 18 U.S.C. § 3121(b)(1).

We believe there is a strong argument that EINSTEIN 2.0 operations are subject to this “rights or property” exception. The rights or property exception in the Pen/Trap Act is more expansive than the parallel provisions in the Wiretap Act and the SCA. There is no requirement under the Pen/Trap Act provision that the action of a provider be “necessary” to protecting its rights or property. Furthermore, the Pen/Trap Act provision also permits a provider to protect not only its own rights or property, but also its users against “abuse of service or unlawful use of service.” 18 U.S.C. § 3121(b)(1). Accordingly, under EINSTEIN 2.0 operations the Government is protecting the Executive Branch “users” of the Internet service and the Government’s own rights and property. For these reasons and the reasons noted with respect to the narrower exception in the Wiretap Act, *see supra* pp. 25-27, we believe the rights or property exception to the Pen/Trap Act provides an additional basis to believe that EINSTEIN 2.0 operations are consistent with the Pen/Trap Act.

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 26

~~TOP SECRET//SI//NOFORN//20320108~~

EXHIBIT B

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

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

98th U.S. COURT OF APPEALS
CLERK OF COURT

(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~~~~TOP SECRET//SI//NOFORN//20320108~~

JA3194

~~TOP SECRET//SI//NOFORN//20310108~~

- (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.

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

(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

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

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

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

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.

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

- (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

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

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.

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

(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

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

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 disseminations 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

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

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

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

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.

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

(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;

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

- (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.

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

(U) Section 8 - Collaboration with Foreign Governments

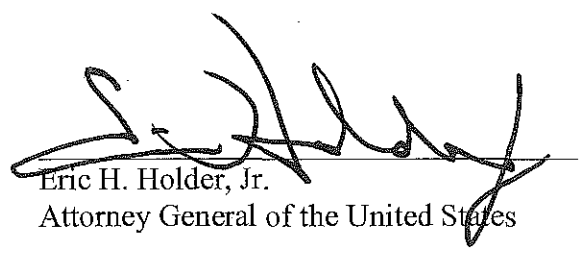
- (a) (U) Procedures for the dissemination of evaluated and minimized information. Pursuant to section 1.7(c)(8) of Executive Order No. 12333, as amended, NSA conducts foreign cryptologic liaison relationships with certain foreign governments. Information acquired pursuant to section 702 of the Act may 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.

~~TOP SECRET//SI//NOFORN//20320108~~

~~TOP SECRET//SI//NOFORN//20310108~~

(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

~~TOP SECRET//SI//NOFORN//20320108~~

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 27

The Guardian



XKeyscore: NSA tool collects 'nearly everything a user does on the internet'

. XKeyscore gives 'widest-reaching' collection of online data . NSA analysts require no prior authorization for searches . Sweeps up emails, social media activity and browsing history . NSA's XKeyscore program - read one of the presentations

Glenn Greenwald

Wed 31 Jul 2013 08.56 EDT

A top secret National Security Agency program allows analysts to search with no prior authorization through vast databases containing emails, online chats and the browsing histories of millions of individuals, according to documents provided by whistleblower Edward Snowden.

The NSA boasts in training materials that the program, called XKeyscore, is its "widest-reaching" system for developing intelligence from the internet.

The latest revelations will add to the intense public and congressional debate around the extent of NSA surveillance programs. They come as senior intelligence officials testify to the Senate judiciary committee on Wednesday, releasing classified documents in response to the Guardian's earlier stories on bulk collection of phone records and Fisa surveillance court oversight.

JA3210

12/16/2018

XKeyscore: NSA tool collects 'nearly everything a user does on the internet' | US news | The Guardian

The files shed light on one of Snowden's most controversial statements, made in his first video interview published by the Guardian on June 10.

"I, sitting at my desk," said Snowden, could "wiretap anyone, from you or your accountant, to a federal judge or even the president, if I had a personal email".

US officials vehemently denied this specific claim. Mike Rogers, the Republican chairman of the House intelligence committee, said of Snowden's assertion: "He's lying. It's impossible for him to do what he was saying he could do."

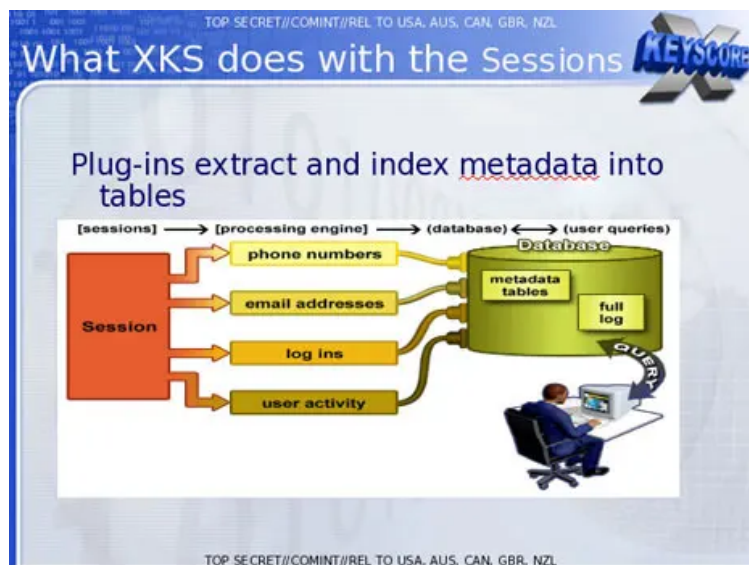
But training materials for XKeyscore detail how analysts can use it and other systems to mine enormous agency databases by filling in a simple on-screen form giving only a broad justification for the search. The request is not reviewed by a court or any NSA personnel before it is processed.

XKeyscore, the documents boast, is the NSA's "widest reaching" system developing intelligence from computer networks - what the agency calls Digital Network Intelligence (DNI). One presentation claims the program covers "nearly everything a typical user does on the internet", including the content of emails, websites visited and searches, as well as their metadata.

Analysts can also use XKeyscore and other NSA systems to obtain ongoing "real-time" interception of an individual's internet activity.

Under US law, the NSA is required to obtain an individualized Fisa warrant only if the target of their surveillance is a 'US person', though no such warrant is required for intercepting the communications of Americans with foreign targets. But XKeyscore provides the technological capability, if not the legal authority, to target even US persons for extensive electronic surveillance without a warrant provided that some identifying information, such as their email or IP address, is known to the analyst.

One training slide illustrates the digital activity constantly being collected by XKeyscore and the analyst's ability to query the databases at any time.



KS1 Photograph: Guardian

The purpose of XKeyscore is to allow analysts to search the metadata as well as the content of emails and other internet activity, such as browser history, even when there is no known email

account (a "selector" in NSA parlance) associated with the individual being targeted.

Analysts can also search by name, telephone number, IP address, keywords, the language in which the internet activity was conducted or the type of browser used.

One document notes that this is because "strong selection [search by email address] itself gives us only a very limited capability" because "a large amount of time spent on the web is performing actions that are anonymous."

The NSA documents assert that by 2008, 300 terrorists had been captured using intelligence from XKeyscore.

Analysts are warned that searching the full database for content will yield too many results to sift through. Instead they are advised to use the metadata also stored in the databases to narrow down what to review.

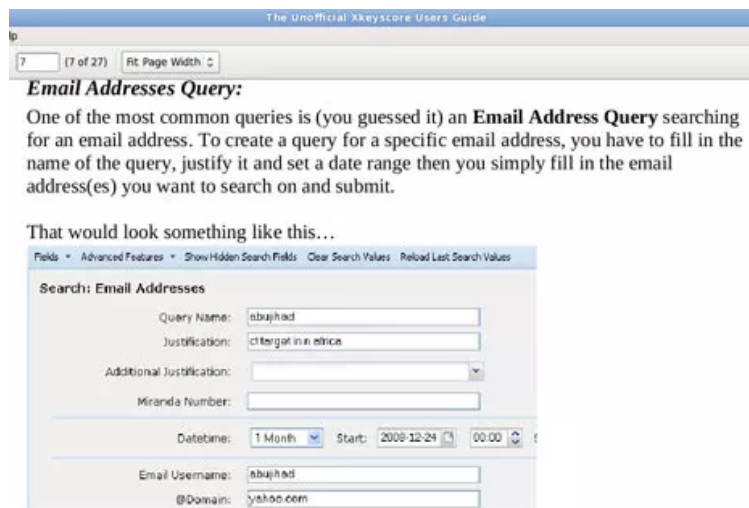
A slide entitled "plug-ins" in a December 2012 document describes the various fields of information that can be searched. It includes "every email address seen in a session by both username and domain", "every phone number seen in a session (eg address book entries or signature block)" and user activity - "the webmail and chat activity to include username, buddylist, machine specific cookies etc".

Email monitoring

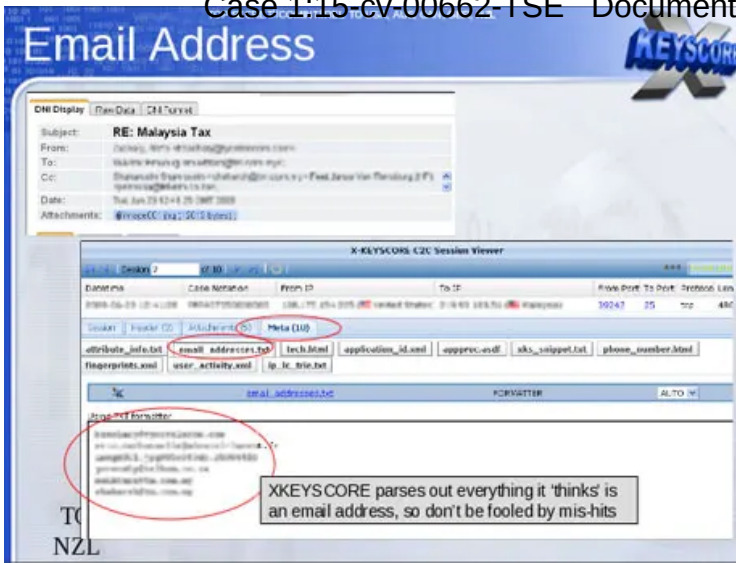
In a second Guardian interview in June, Snowden elaborated on his statement about being able to read any individual's email if he had their email address. He said the claim was based in part on the email search capabilities of XKeyscore, which Snowden says he was authorized to use while working as a Booz Allen contractor for the NSA.

One top-secret document describes how the program "searches within bodies of emails, webpages and documents", including the "To, From, CC, BCC lines" and the 'Contact Us' pages on websites".

To search for emails, an analyst using XKS enters the individual's email address into a simple online search form, along with the "justification" for the search and the time period for which the emails are sought.



KS2 Photograph: Guardian

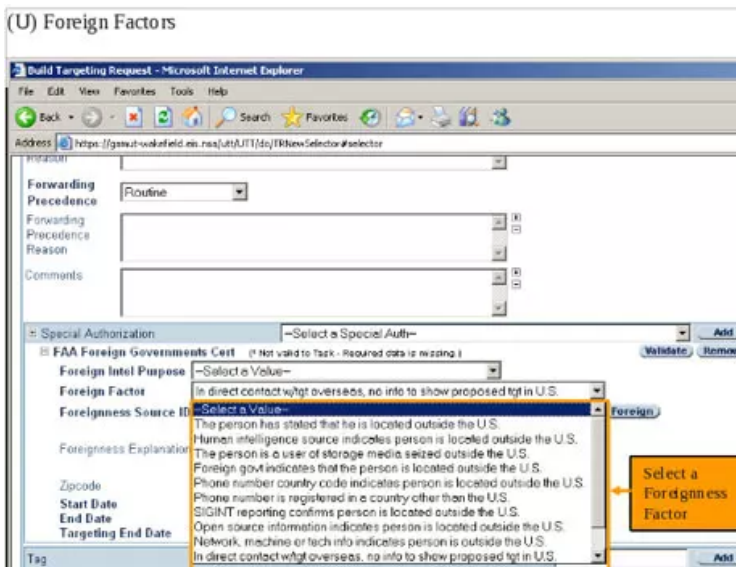


KS3edit2 Photograph: Guardian

The analyst then selects which of those returned emails they want to read by opening them in NSA reading software.

The system is similar to the way in which NSA analysts generally can intercept the communications of anyone they select, including, as one NSA document put it, "communications that transit the United States and communications that terminate in the United States".

One document, a top secret 2010 guide describing the training received by NSA analysts for general surveillance under the Fisa Amendments Act of 2008, explains that analysts can begin surveillance on anyone by clicking a few simple pull-down menus designed to provide both legal and targeting justifications. Once options on the pull-down menus are selected, their target is marked for electronic surveillance and the analyst is able to review the content of their communications:



KS4 Photograph: Guardian

Chats, browsing history and other internet activity

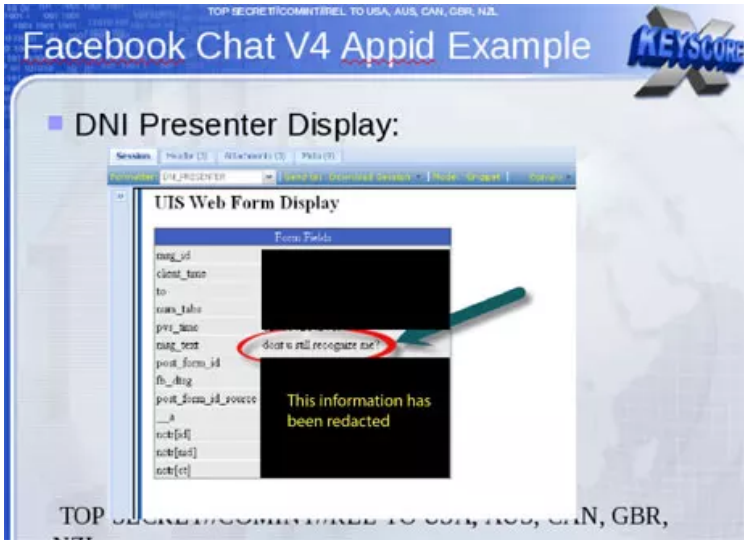
Beyond emails, the XKeyscore system allows analysts to monitor a virtually unlimited array of other internet activities, including those within social media.

12/16/2018

XKeyscore: NSA tool collects 'nearly everything a user does on the internet' | US news | The Guardian

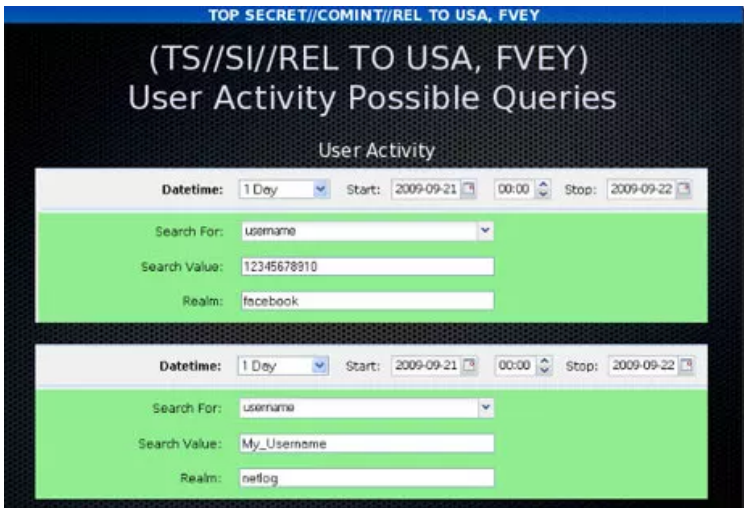
Case 1:15-cv-00662-TSE Document 168-31 Filed 12/18/18 Page 6 of 11

An NSA tool called DNI Presenter, used to read the content of stored emails, also enables an analyst using XKeyscore to read the content of Facebook chats or private messages.



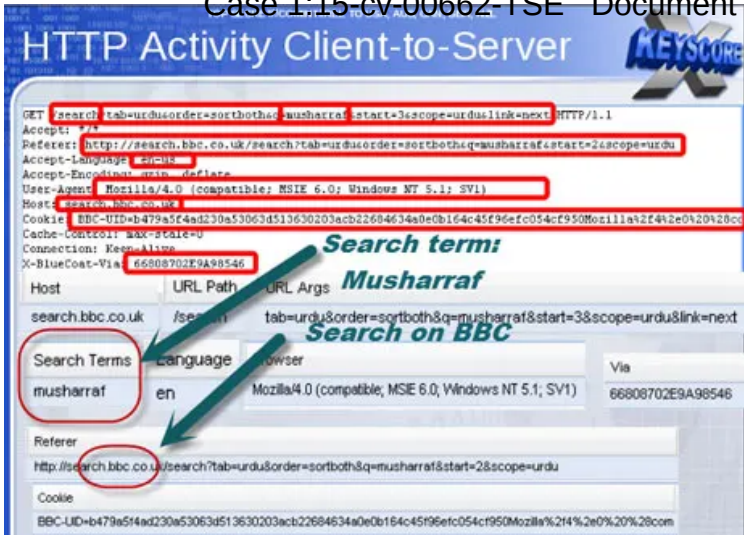
KS55edit Photograph: Guardian

An analyst can monitor such Facebook chats by entering the Facebook user name and a date range into a simple search screen.



KS6 Photograph: Guardian

Analysts can search for internet browsing activities using a wide range of information, including search terms entered by the user or the websites viewed.



KS7 Photograph: Guardian

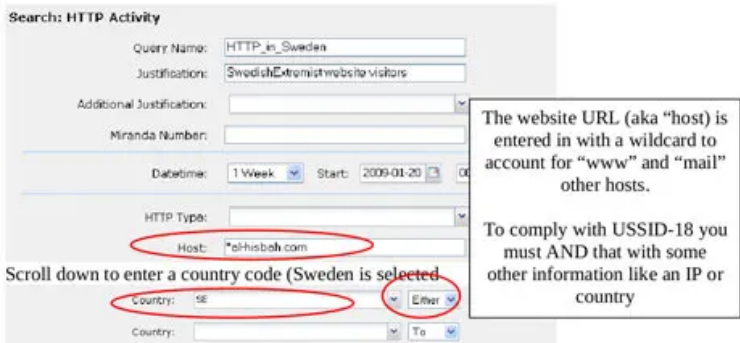
As one slide indicates, the ability to search HTTP activity by keyword permits the analyst access to what the NSA calls "nearly everything a typical user does on the internet".



KS8 Photograph: Guardian

The XKeyscore program also allows an analyst to learn the IP addresses of every person who visits any website the analyst specifies.

1. If you know the particular website the target visits. For this example, I'm looking for everyone in Sweden that visits a particular extremist web forum.



KS9 Photograph: Guardian

12/16/2018

XKeyscore: NSA tool collects 'nearly everything a user does on the internet' | US news | The Guardian

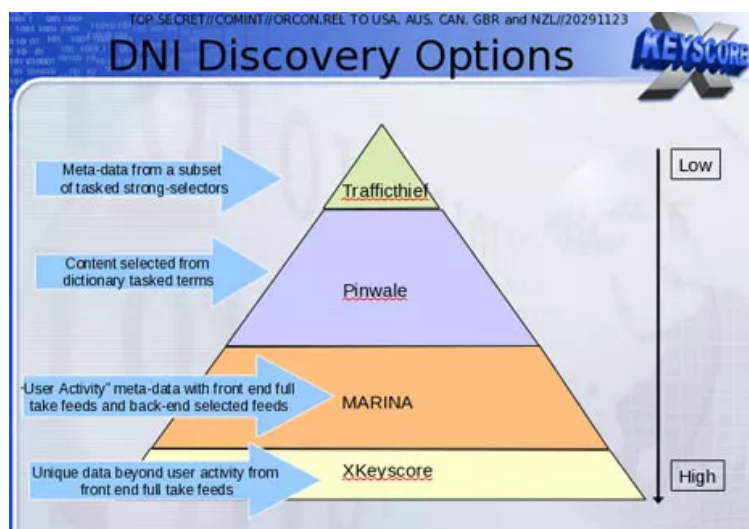
The quantity of communications accessible through programs such as XKeyscore is staggeringly large. One NSA report from 2007 estimated that there were 850bn "call events" collected and stored in the NSA databases, and close to 150bn internet records. Each day, the document says, 1-2bn records were added.

William Binney, a former NSA mathematician, said last year that the agency had "assembled on the order of 20tn transactions about US citizens with other US citizens", an estimate, he said, that "only was involving phone calls and emails". A 2010 Washington Post article reported that "every day, collection systems at the [NSA] intercept and store 1.7bn emails, phone calls and other type of communications."

The XKeyscore system is continuously collecting so much internet data that it can be stored only for short periods of time. Content remains on the system for only three to five days, while metadata is stored for 30 days. One document explains: "At some sites, the amount of data we receive per day (20+ terabytes) can only be stored for as little as 24 hours."

To solve this problem, the NSA has created a multi-tiered system that allows analysts to store "interesting" content in other databases, such as one named Pinwale which can store material for up to five years.

It is the databases of XKeyscore, one document shows, that now contain the greatest amount of communications data collected by the NSA.



KS10 Photograph: Guardian

In 2012, there were at least 41 billion total records collected and stored in XKeyscore for a single 30-day period.

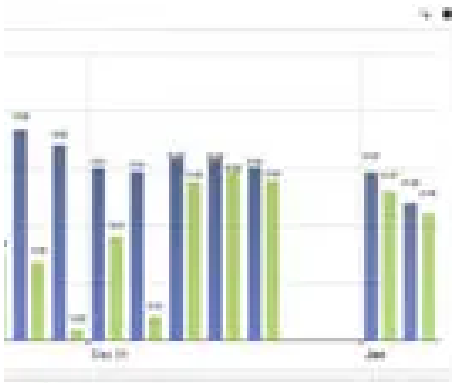
Legal v technical restrictions

While the Fisa Amendments Act of 2008 requires an individualized warrant for the targeting of US persons, NSA analysts are permitted to intercept the communications of such individuals without a warrant if they are in contact with one of the NSA's foreign targets.

The ACLU's deputy legal director, Jameel Jaffer, told the Guardian last month that national security officials expressly said that a primary purpose of the new law was to enable them to collect large amounts of Americans' communications without individualized warrants.

12/16/2018

XKeyscore: NSA tool collects 'nearly everything a user does on the internet' | US news | The Guardian



XKEYSCORE
 47,995,304,143
 Records

"The government doesn't need to 'target' Americans in order to collect huge volumes of their communications," said Jaffer. "The government inevitably sweeps up the communications of many Americans" when targeting foreign nationals for surveillance.

An example is provided by one XKeyscore document showing an NSA target in Tehran communicating with people in Frankfurt, Amsterdam and New York.

TOP SECRET//COMINT//REL TO USA, AUK, CAN, GBR, JAL

Example #2

- Full Log table contains the standard DNI meta-data with *some but not all* information from other plug-ins included (ie. Username from User Activity and Application Info contains some HTTP activity)

Application Info	Username	From (Country, To (City)	Date/Time	From IP	To IP	Filter
http://update.nsl.com/Products.Cc		TEHRAN US NEWYORK	2009-05-20 18:05:41	2009-05-20 00:00:16		3842 00
http://platform.fb.facebook.com/v	narges.arastode@gmail.com	TEHRAN DE FRANKFURT	2009-05-20 18:05:41	2009-05-20 00:00:16		4201 00
http://platform.fb.facebook.com/v	narges.arastode@gmail.com	TEHRAN DE FRANKFURT	2009-05-20 18:05:41	2009-05-20 00:00:16		4201 00
http://platform.fb.facebook.com/v	narges.arastode@gmail.com	TEHRAN DE FRANKFURT	2009-05-20 18:05:41	2009-05-20 00:00:16		4201 00
http://news.us.af.mil/afnews		TEHRAN GB LONDON	2009-05-20 18:05:41	2009-05-20 00:00:16		37403 00
http://b.state.ak.fbcdn.net/track		TEHRAN DE FRANKFURT	2009-05-20 18:05:41	2009-05-20 00:00:16		41972 00
http://b.state.ak.fbcdn.net/track		TEHRAN DE FRANKFURT	2009-05-20 18:05:41	2009-05-20 00:00:16		41972 00
http://platform.fb.facebook.com/v	narges.arastode@gmail.com	TEHRAN DE FRANKFURT	2009-05-20 18:05:41	2009-05-20 00:00:16		4044 00
http://photos-ak.fbcdn.net/phot		TEHRAN NL AMSTERDAM	2009-05-20 18:05:41	2009-05-20 00:00:16		41631 00
http://photos-ak.fbcdn.net/phot		TEHRAN NL AMSTERDAM	2009-05-20 18:05:41	2009-05-20 00:00:16		41631 00

IP addresses redacted

KS12 Photograph: Guardian

In recent years, the NSA has attempted to segregate exclusively domestic US communications in separate databases. But even NSA documents acknowledge that such efforts are imperfect, as even purely domestic communications can travel on foreign systems, and NSA tools are sometimes unable to identify the national origins of communications.

Moreover, all communications between Americans and someone on foreign soil are included in the same databases as foreign-to-foreign communications, making them readily searchable without warrants.

Some searches conducted by NSA analysts are periodically reviewed by their supervisors within the NSA. "It's very rare to be questioned on our searches," Snowden told the Guardian in June, "and even when we are, it's usually along the lines of: 'let's bulk up the justification!'"

In a letter this week to senator Ron Wyden, director of national intelligence James Clapper acknowledged that NSA analysts have exceeded even legal limits as interpreted by the NSA in domestic surveillance.

Acknowledging what he called "a number of compliance problems", Clapper attributed them to "human error" or "highly sophisticated technology issues" rather than "bad faith".

However, Wyden said on the Senate floor on Tuesday: "These violations are more serious than those stated by the intelligence community, and are troubling."

In a statement to the Guardian, the NSA said: "NSA's activities are focused and specifically deployed against - and only against - legitimate foreign intelligence targets in response to requirements that our leaders need for information necessary to protect our nation and its interests."

"XKeyscore is used as a part of NSA's lawful foreign signals intelligence collection system."

"Allegations of widespread, unchecked analyst access to NSA collection data are simply not true. Access to XKeyscore, as well as all of NSA's analytic tools, is limited to only those personnel who require access for their assigned tasks ... In addition, there are multiple technical, manual and supervisory checks and balances within the system to prevent deliberate misuse from occurring."

"Every search by an NSA analyst is fully auditable, to ensure that they are proper and within the law."

"These types of programs allow us to collect the information that enables us to perform our missions successfully - to defend the nation and to protect US and allied troops abroad."

\$0
contributed
\$0
our goal

In these critical times ...

... Guardian columnist and author Rebecca Solnit urges you to show your support for independent journalism with a year-end gift to The Guardian. We are asking our US readers to help us raise \$1 million dollars by the new year to report on the most important stories in 2019.

A note from Rebecca:

"First they came for the journalists," said the young man's sign. "We don't know what happened after that." It's a brilliant comment that underscores two things. One is how utterly necessary it is to a free, powerful, informed public, to have the ability to act on what happens beyond our own horizon, to make choices about our governments whether by blockading a senate or parliament or electing people we've learned about from the news.

The other is how much tyrants and would-be tyrants fear a free press - and what your enemies think is often the best way to measure whether you matter. They know autocracy depend on keeping the public ignorant on some fronts and misinformed on others.

We've seen direct attacks on journalists in the past year, from the murder of Jamal Khashoggi to Trump's incessant attacks on the media as "the enemy of the people," and for a couple of decades we've seen the indirect attacks that are Silicon Valley's siphoning off of advertising revenue and amplification of untruths for profit.

It costs a lot to send someone out to cover a campaign or to investigate a crime; it's hard work that requires expertise and support from our readers. This year, The Guardian has covered everything from tech to feminism to Trump to fossil fuel politics. It is our editorial independence that has

12/16/2018

XKeyscore: NSA tool collects 'nearly everything a user does on the internet' | US news | The Guardian

Case 1:15-cv-00662-TSE Document 168-31 Filed 12/18/18 Page 11 of 11

allowed us to deliver this fearless reporting; an independence that's sometimes hard to find in other US-based media. We hope you appreciate our efforts.

We want to say a huge thank you to everyone who has supported The Guardian so far. We hope to pass our goal by early January 2019. Every contribution, big or small, will help us reach it. **Please make a year-end gift today to show your ongoing support for our independent journalism. Thank you.**

Support The Guardian



Topics

- The NSA files
- Glenn Greenwald on security and liberty
- Surveillance
- NSA
- Privacy
- Internet
- Data protection
- US politics
- news

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 28

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



JA3221

Google
Earth

@mail.ru

Gmail
by Google

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 29

The Intercept

XKEYSCORE

NSA's Google for the World's Private Communications



Morgan Marquis-Boire, Glenn Greenwald, Micah Lee

July 1 2015, 10:49 a.m.

One of the National Security Agency's most powerful tools of mass surveillance makes tracking someone's Internet usage as easy as entering an email address, and provides no built-in technology to prevent abuse. Today, *The Intercept* is publishing 48 top-secret and other classified documents about XKEYSCORE dated up to 2013, which shed new light on the breadth, depth and functionality of this critical spy system – one of the largest releases yet of documents provided by NSA whistleblower Edward Snowden.

The NSA's XKEYSCORE program, first [revealed](#) by *The Guardian*, sweeps up countless people's Internet searches, emails, documents, usernames and passwords, and other private communications. XKEYSCORE is fed a constant flow of Internet traffic from [fiber optic cables](#) that make up the backbone of the world's communication network, among other sources, for processing. As of 2008, the surveillance system boasted approximately 150 field sites in the United States, Mexico, Brazil, United Kingdom, Spain, Russia, Nigeria, Somalia, Pakistan, Japan, Australia, as well as many other countries, consisting of over 700 servers.

12/16/2018

XKEYSCORE: NSA's Google for the World's Private Communications

Case 1:15-cv-00662-TSE Document 168-33 Filed 12/18/18 Page 3 of 15

These servers store “full-take data” at the collection sites – meaning that they captured all of the traffic collected – and, as of 2009, stored content for 3 to 5 days and metadata for 30 to 45 days. NSA documents indicate that tens of billions of records are stored in its database. “It is a fully distributed processing and query system that runs on machines around the world,” an NSA briefing on XKEYSCORE says. “At field sites, XKEYSCORE can run on multiple computers that gives it the ability to scale in both processing power and storage.”

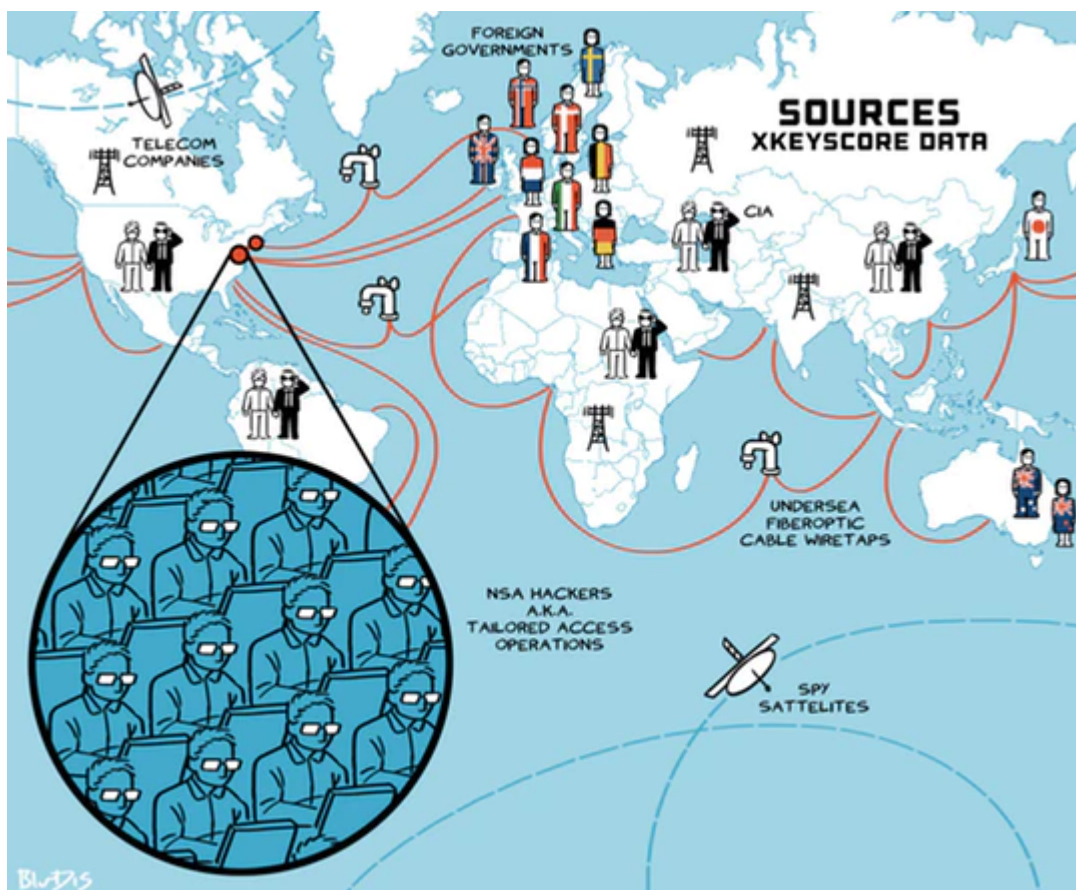


Illustration: Blue Delliquanti and David Axe for The Intercept

XKEYSCORE also collects and processes Internet traffic from Americans, though NSA analysts are taught to avoid querying the system in ways that might result in spying on U.S. data. Experts and privacy activists, however, have long doubted that such exclusions are effective in preventing large amounts of American data from being swept up. One document *The Intercept* is publishing today suggests that FISA warrants

have authorized “full-take” collection of traffic from at least some U.S. web forums.

The system is not limited to collecting web traffic. The 2013 document, “VoIP Configuration and Forwarding Read Me,” details how to forward VoIP data from XKEYSCORE into NUCLEON, NSA’s repository for voice intercepts, facsimile, video and “pre-released transcription.” At the time, it supported more than 8,000 users globally and was made up of 75 servers absorbing 700,000 voice, fax, video and tag files per day.

The reach and potency of XKEYSCORE as a surveillance instrument is astonishing. The *Guardian* report noted that NSA itself refers to the program as its “widest reaching” system. In February of this year, *The Intercept* reported that NSA and GCHQ hacked into the internal network of Gemalto, the world’s largest provider of cell phone SIM cards, in order to steal millions of encryption keys used to protect the privacy of cell phone communication. XKEYSCORE played a vital role in the spies’ hacking by providing government hackers access to the email accounts of Gemalto employees.

Numerous key NSA partners, including Canada, New Zealand and the U.K., have access to the mass surveillance databases of XKEYSCORE. In March, the *New Zealand Herald*, in partnership with *The Intercept*, revealed that the New Zealand government used XKEYSCORE to spy on candidates for the position of World Trade Organization director general and also members of the *Solomon Islands government*.

These newly published documents demonstrate that collected communications not only include emails, chats and web-browsing traffic, but also pictures, documents, voice calls, webcam photos, web searches, advertising analytics traffic, social media traffic, botnet traffic, logged keystrokes, computer network exploitation (CNE) targeting, intercepted username and password pairs, file uploads to online services, Skype sessions and more.

Bulk collection and population surveillance

XKEYSCORE allows for incredibly broad surveillance of people based on perceived patterns of suspicious behavior. It is possible, for instance, to query the system to show the activities of people based on their location, nationality and websites visited. For instance, one slide displays the search “germansinpakistn,” showing an analyst querying XKEYSCORE for all [individuals in Pakistan visiting specific German language message boards](#).

As sites like Twitter and Facebook become increasingly significant in the world’s day-to-day communications (a Pew study [shows](#) that 71 percent of online adults in the U.S. use Facebook), they become a critical source of surveillance data. Traffic from popular social media sites is described as “a great starting point” for tracking individuals, according to an XKEYSCORE [presentation](#) titled “Tracking Targets on Online Social Networks.”

When intelligence agencies collect massive amounts of Internet traffic all over the world, they face the challenge of making sense of that data. The vast quantities collected make it difficult to connect the stored traffic to specific individuals.

Internet companies have also encountered this problem and have solved it by tracking their users with identifiers that are unique to each individual, often in the form of browser cookies. Cookies are small pieces of data that websites store in visitors’ browsers. They are used for a variety of purposes, including authenticating users (cookies make it possible to log in to websites), storing preferences, and uniquely tracking individuals even if they’re using the same IP address as many other people. Websites also embed code used by third-party services to

12/16/2018

XKEYSCORE: NSA's Google for the World's Private Communications

Case 1:15-cv-00662-TSE Document 168-33 Filed 12/18/18 Page 6 of 15
collect analytics or host ads, which also use cookies to track users.

According to [one slide](#), "Almost all websites have cookies enabled."

The NSA's ability to piggyback off of private companies' tracking of their own users is a vital instrument that allows the agency to trace the data it collects to individual users. It makes no difference if visitors switch to public Wi-Fi networks or connect to VPNs to change their IP addresses: the tracking cookie will follow them around as long as they are using the same web browser and fail to clear their cookies.

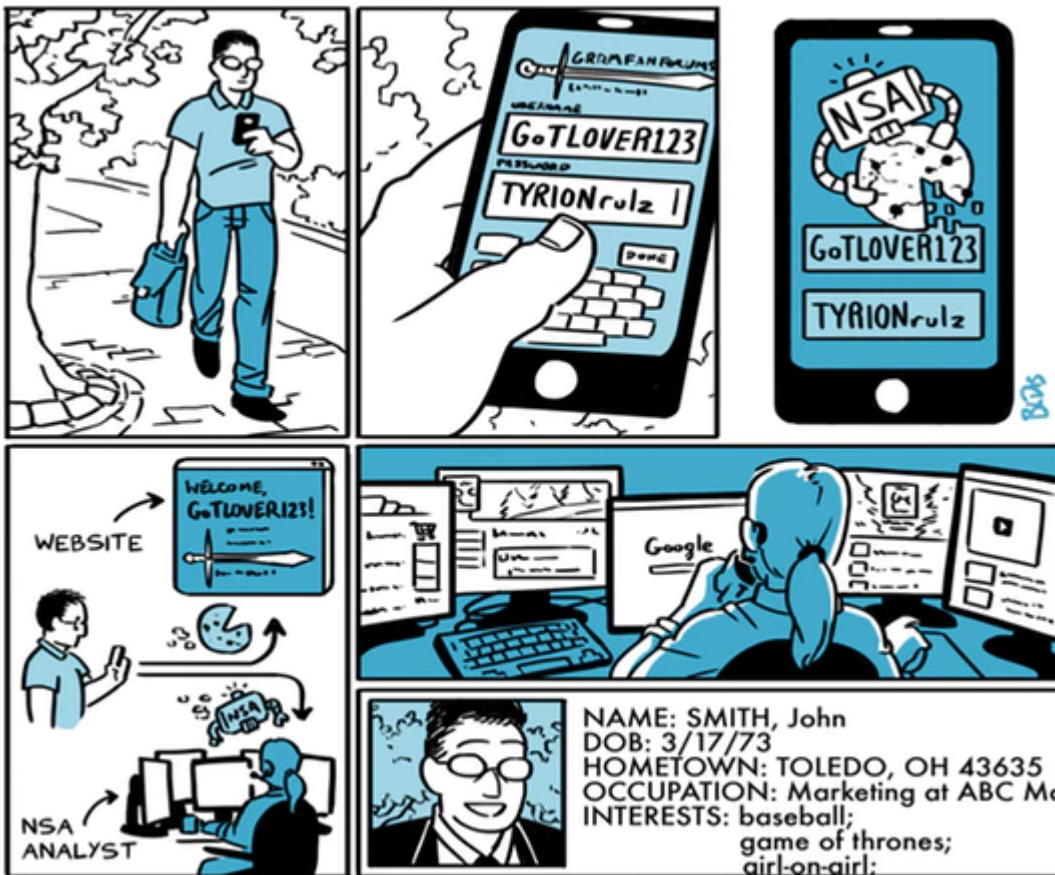


Illustration: Blue Delliquanti and David Axe for The Intercept

Apps that run on tablets and smartphones also use analytics services that uniquely track users. Almost every time a user sees an advertisement (in an app or in a web browser), the ad network is tracking users in the same way. A [secret GCHQ and CSE program called BADASS](#), which is similar to XKEYSCORE but with a much narrower scope, mines as much valuable information from leaky smartphone

JA3227

apps as possible, including unique tracking identifiers that app developers use to track their own users. In May of this year, CBC, in partnership with *The Intercept*, [revealed](#) that XKEYSCORE was used to track smartphone connections to the app marketplaces run by Samsung and Google. Surveillance agency analysts also use other types of traffic data that gets scooped into XKEYSCORE to track people, such as [Windows crash reports](#).

In a statement to *The Intercept*, the NSA reiterated its position that such sweeping surveillance capabilities are needed to fight the War on Terror:

“The U.S. Government calls on its intelligence agencies to protect the United States, its citizens, and its allies from a wide array of serious threats. These threats include terrorist plots from al-Qaeda, ISIL, and others; the proliferation of weapons of mass destruction; foreign aggression against the United States and our allies; and international criminal organizations.”

Indeed, one of the specific examples of XKEYSCORE applications given in the documents is spying on Shaykh Atiyatallah, an al Qaeda senior leader and Osama bin Laden confidant. A few years before his death, Atiyatallah did what many people have often done: He googled himself. He searched his various aliases, an associate and the name of his book. As he did so, all of that information was captured by XKEYSCORE.

XKEYSCORE has, however, also been used to spy on non-terrorist targets. The April 18, 2013 issue of the internal NSA publication *Special Source Operations Weekly* [boasts](#) that analysts were successful in using XKEYSCORE to obtain U.N. Secretary General Ban Ki-moon’s talking points prior to a meeting with President Obama.



Illustration: Blue Delliquanti and David Axe for The Intercept

XKEYSCORE for hacking: Easily collecting user names, passwords and much more

XKEYSCORE plays a central role in how the U.S. government and its surveillance allies hack computer networks around the world. One top-secret 2009 NSA document describes how the system is used by the NSA to gather information for the Office of Tailored Access Operations, an NSA division responsible for Computer Network Exploitation (CNE) – i.e., targeted hacking.

Particularly in 2009, the hacking tactics enabled by XKEYSCORE would have yielded significant returns as use of encryption was less widespread than today. Jonathan Brossard, a security researcher and the

CEO of Toucan Systems, told *The Intercept*: “Anyone could be trained to do this in less than one day: they simply enter the name of the server they want to hack into XKEYSCORE, type enter, and are presented login and password pairs to connect to this machine. Done. Finito.” [Previous reporting](#) by *The Intercept* revealed that systems administrators are a popular target of the NSA. “Who better to target than the person that already has the ‘keys to the kingdom?’” read a 2012 post on an internal NSA discussion board.

This system enables analysts to access web mail servers with [remarkable ease](#).

The same methods are used to steal the credentials – user names and passwords – of individual users of [message boards](#).

[Hacker forums](#) are also monitored for people selling or using exploits and other hacking tools. While the NSA is clearly monitoring to understand the capabilities developed by its adversaries, it is also monitoring locations where such capabilities can be purchased.

Other information gained via XKEYSCORE facilitates the remote exploitation of target computers. By extracting browser fingerprint and operating system versions from Internet traffic, the system allows analysts to quickly assess the [exploitability of a target](#). Brossard, the security researcher, said that “NSA has built an impressively complete set of automated hacking tools for their analysts to use.”

Given the breadth of information collected by XKEYSCORE, accessing and exploiting a target’s online activity is a matter of a few mouse clicks. Brossard explains: “The amount of work an analyst has to perform to actually break into remote computers over the Internet seems ridiculously reduced – we are talking minutes, if not seconds. Simple. As easy as typing a few words in Google.”

These facts bolster one of Snowden's most controversial statements, made in his [first video interview published by *The Guardian*](#) on June 9, 2013. "I, sitting at my desk," said Snowden, could "wiretap anyone, from you or your accountant, to a federal judge to even the president, if I had a personal email."

Indeed, training documents for XKEYSCORE repeatedly highlight how user-friendly the program is: with just a few clicks, any analyst with access to it can conduct sweeping searches simply by entering a person's email address, telephone number, name or other identifying data. There is no indication in the documents reviewed that prior approval is needed for specific searches.

In addition to login credentials and other target intelligence, XKEYSCORE collects [router configuration information](#), which it shares with Tailored Access Operations. The office is able to exploit routers and then feed the traffic traveling through those routers into their collection infrastructure. This allows the NSA to spy on traffic from otherwise out-of-reach networks. XKEYSCORE documents reference router configurations, and [a document previously published by *Der Spiegel*](#) shows that "active implants" can be used to "cop[y] traffic and direc[t]" it past a passive collector.

XKEYSCORE for counterintelligence

Beyond enabling the collection, categorization, and querying of metadata and content, XKEYSCORE has also been used to monitor the surveillance and hacking actions of foreign nation states and to gather the fruits of their hacking. *The Intercept* [previously reported](#) that NSA and its allies spy on hackers in order to collect what they collect.

Once the hacking tools and techniques of a foreign entity (for instance, [South Korea](#)) are identified, analysts can then extract the country's espionage targets from XKEYSCORE, and gather information that the foreign power has managed to steal.

Monitoring of foreign state hackers could allow the NSA to gather techniques and tools used by foreign actors, including knowledge of zero-day exploits – software bugs that allow attackers to hack into systems, and that not even the software vendor knows about – and implants. Additionally, by monitoring vulnerability reports sent to vendors such as [Kaspersky](#), the agency could learn when exploits they were actively using need to be retired because they've been discovered by a third party.

Seizure v. searching: Oversight, audit trail and the Fourth Amendment

By the nature of how it sweeps up information, XKEYSCORE gathers communications of Americans, despite the Fourth Amendment protection against “unreasonable search and seizure” – including searching data without a warrant. The NSA says it does not target U.S. citizens' communications without a warrant, but acknowledges that it “incidentally” collects and reads some of it without one, minimizing the information that is retained or shared.

But that interpretation of the law is dubious at best.

XKEYSCORE training documents say that the “burden is on user/auditor to comply with USSID-18 or other rules,” apparently including the British Human Rights Act (HRA), which protects the rights of U.K. citizens. U.S. Signals Intelligence Directive 18 (USSID 18) is the American directive that governs “U.S. person minimization.”

Kurt Opsahl, the Electronic Frontier Foundation's general counsel, describes USSID 18 as "an attempt by the intelligence community to comply with the Fourth Amendment. But it doesn't come from a court, it comes from the executive."

If, for instance, an analyst searched XKEYSCORE for all iPhone users, this query would [violate USSID 18](#) due to the inevitable American iPhone users that would be grabbed without a warrant, as the NSA's own training materials make clear.

Opsahl believes that analysts are not prevented by technical means from making queries that violate USSID 18. "The document discusses whether auditors will be happy or unhappy. This indicates that compliance will be achieved by after-the-fact auditing, not by preventing the search."

Screenshots of the XKEYSCORE web-based user interface included in slides show that analysts see a prominent warning message: "This system is audited for USSID 18 and Human Rights Act compliance." When analysts log in to the system, they see a more detailed message warning that "an audit trail has been established and will be searched" in response to HRA complaints, and as part of the USSID 18 and USSID 9 audit process.

Because the XKEYSCORE system does not appear to prevent analysts from making queries that would be in violation of these rules, Opsahl concludes that "there's a tremendous amount of power being placed in the hands of analysts." And while those analysts may be subject to audits, "at least in the short term they can still obtain information that they shouldn't have."

During a [symposium](#) in January 2015 hosted at Harvard University, Edward Snowden, who spoke via video call, said that NSA analysts are "completely free from any meaningful oversight." Speaking about the

people who audit NSA systems like XKEYSCORE for USSID 18

compliance, he said, “The majority of the people who are doing the auditing are the friends of the analysts. They work in the same office. They’re not full-time auditors, they’re guys who have other duties assigned. There are a few traveling auditors who go around and look at the things that are out there, but really it’s not robust.”

In a statement to *The Intercept*, the NSA said:

“The National Security Agency’s foreign intelligence operations are 1) authorized by law; 2) subject to multiple layers of stringent internal and external oversight; and 3) conducted in a manner that is designed to protect privacy and civil liberties. As provided for by Presidential Policy Directive 28 (PPD-28), all persons, regardless of their nationality, have legitimate privacy interests in the handling of their personal information. NSA goes to great lengths to narrowly tailor and focus its signals intelligence operations on the collection of communications that are most likely to contain foreign intelligence or counterintelligence information.”

Coming next: A Look at the Inner Workings of XKEYSCORE

Source maps: XKS as a SIGDEV Tool, p. 15, and XKS Intro, p. 6

Documents published with this article:

- [Advanced HTTP Activity Analysis](#)
- [Analyzing Mobile Cellular DNI in XKS](#)
- [ASFD Readme](#)
- [CADENCE Readme](#)
- [Category Throttling](#)
- [CNE Analysis in XKS](#)
- [Comms Readme](#)

- [DEEPDIVE Readme](#)
- [DNI101](#)
- [Email Address vs User Activity](#)
- [Free File Uploaders](#)
- [Finding and Querying Document Metadata](#)
- [Full Log vs HTTP](#)
- [Guide to Using Contexts in XKS Fingerprints](#)
- [HTTP Activity in XKS](#)
- [HTTP Activity vs User Activity](#)
- [Intro to Context Sensitive Scanning With XKS Fingerprints](#)
- [Intro to XKS AppIDs and Fingerprints](#)
- [OSINT Fusion Project](#)
- [Phone Number Extractor](#)
- [RWC Updater Readme](#)
- [Selection Forwarding Readme](#)
- [Stats Config Readme](#)
- [Tracking Targets on Online Social Networks](#)
- [TRAFFICTHIEF Readme](#)
- [Unofficial XKS User Guide](#)
- [User Agents](#)
- [Using XKS to Enable TAO](#)
- [UTT Config Readme](#)
- [VOIP in XKS](#)
- [VOIP Readme](#)
- [Web Forum Exploitation Using XKS](#)
- [Writing XKS Fingerprints](#)
- [XKS Application IDs](#)
- [XKS Application IDs Brief](#)
- [XKS as a SIGDEV Tool](#)
- [XKS, Cipher Detection, and You!](#)
- [XKS for Counter CNE](#)
- [XKS Intro](#)

- [XKS Logos Embedded in Docs](#)
- [XKS Search Forms](#)
- [XKS System Administration](#)
- [XKS Targets Visiting Specific Websites](#)
- [XKS Tech Extractor 2009](#)
- [XKS Tech Extractor 2010](#)
- [XKS Workflows 2009](#)
- [XKS Workflows 2011](#)
- [UN Secretary General XKS](#)



We depend on the support of readers like you to help keep our nonprofit newsroom strong and independent. [Join Us](#) →

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 30

TOP SECRET//COMINT//REL TO USA, FVEY



XKEYSCORE for Counter-CNE

"Using the XKS CNE dataset and a DISGRUNTLEDDUCK fingerprint, we now see at least 21 TAO boxes with evidence of this intrusion set, most of which are associated with projects aimed at Iran WMD targets." -- MHS, July 2010

March, 2011

[REDACTED]
xks-cne@r1.r.nsa

TOP SECRET//COMINT//REL TO USA, FVEY

UNCLASSIFIED//FOUO

Overall Classification



The overall classification of this presentation is:

TOP SECRET//COMINT//REL TO USA, FVEY

UNCLASSIFIED//FOUO

SECRET//COMINT//REL TO USA, FVEY

What is XKEYSCORE?



- A suite of software running on a Linux host
- *Classically*, used for DNI processing, selection and survey
- A distributed hierarchy of servers at field sites and headquarters
 - Extract and tag metadata & content from traffic
 - Servicing analyst queries and workflows
- Web and programmatic front-ends

SECRET//COMINT//REL TO USA, FVEY

What is XKEYSCORE?



- A suite of software running on a Linux host
- *Classically*, used for DNI processing, selection and survey
- A distributed hierarchy of servers at field sites and headquarters
 - Extract and tag metadata & content from traffic
 - Servicing analyst queries and workflows
- Web and programmatic front-ends

TOP SECRET//COMINT//REL TO USA, FVEY

XKEYSCORE GUI



XK Metaviewer: shared by f610065:Category Hits at 67D - Mozilla Firefox

https://xks-central.corp.nsa.ic.gov:8143/XKEYSCORE/search/standardsearchformysearch:Home.do

ESS1377: SIDToday for 1/24... | Elthernet - Wikipedia, the free... | My Signatures | XK Metaviewer: shared by r... | XKEYSCORE - For Analysts...

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

XKEYSCORE Welcome [redacted] Log Out

Home Admin Users Search Workflow Control Results Fingerprints Statistics Map My Account XKI drum

Navigation Filter

- Search Wizard
- CNF
 - Email Addresses
 - Extracted Files
 - Full Log DNI
 - Keylogger
 - Machine Information
 - Network Information
 - Registry
- Classic
 - MultiSearch
 - Classic AM
 - Alert
 - BlackBerry
 - Call Logs
 - Category DNI
 - Cellular DNI
 - Cisco Passwords
 - Clamant
 - DNS
 - Document Metadata
 - Document Tagging
 - Email Addresses
 - Extracted Files
 - Full Log DNI
 - Gen Inf
 - HTTP Activity
 - KE Parser
 - Keylogger
 - Logins and Passwords

Histogram Grid

Page 1 of 1

Filter: Fri Port Count

<input checked="" type="checkbox"/>	2304	174
-------------------------------------	------	-----

shared by f610065:Category Hit...

Hold Actions Reports View Map View FILTERS

From	Siged	Active User	Case notation	From IP	To IP	From Port	To Port	From Country (IP)	From City (IP)	From Latitude (IP)	From Longitude (IP)	To Country (IP)	To City (IP)	To Latitude (IP)	To Longitude (IP)
IFTNCOI	US-967D		UA2AA00CB	57	57	2304	2521	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88	2.27
IETTICOI	US-967D		UA2AA00CB	57	57	2304	1679	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88	2.27
ILINCOI	US-067D		UA2AA00CB	57	57	2304	3190	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88	2.27
IETTICOI	US-967D		UA2AA00CB	57	57	2304	1655	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88	2.27
IETTICOI	US-067D		UA2AA00CB	57	57	2304	1120	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88	2.27
IFTNCOI	US-967D		UA2AA00CB	57	57	2304	1130	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88	2.27
IETTICOI	US-967D		UA2AA00CB	57	57	2304	1679	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88	2.27
ILINCOI	US-067D		UA2AA00CB	57	57	2304	2580	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88	2.27
IETTICOI	US-967D		UA2AA00CB	57	57	2304	3190	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88	2.27
ILINCOI	US-067D		UA2AA00CB	57	57	2304	1120	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88	2.27
IFTNCOI	US-967D		UA2AA00CB	57	57	2304	1600	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88	2.27
IETTICOI	US-967D		UA2AA00CB	57	57	2304	1608	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88	2.27
ILINCOI	US-067D		UA2AA00CB	57	57	2304	3050	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88	2.27
IETTICOI	US-967D		UA2AA00CB	57	57	2304	1063	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88	2.27

Page 1 of 6 Page Size: 30 (Max: 100 rows per page)

Displaying 1 - 30 of 174

saved 80219757099313

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Done

TOP SECRET//COMINT//REL TO USA, FVEY

TOP SECRET//COMINT//REL TO USA, FVEY

Example Search



- Let's try a search for suspicious stuff...

http_activity search, 5-eyes defeat, look for fingerprints:

`ndist/discovery/heuristic/BHAM/get_with_content or http/get/with_content`

- While the search runs, some gotchas:
 - You choose where your query is run
 - Content and metadata age-off
 - Burden is on user/auditor to comply with USSID-18 or other rules
 - Geolocation based on IP

TOP SECRET//COMINT//REL TO USA, FVEY

SECRET//COMINT//REL TO USA, FVEY

Search Results



XK Session Viewer - Mozilla Firefox

File Edit View History Bookmarks Tools Help

ic.gov https://xks-central.corp.nsa.ic.gov:8443/XKEYSCORE/layouts/popOutLayout.jsp?pageTitle=Session+Viewer&rowUrl=%2F

This system is audited for USSID 18 and Human Rights Act compliance
CLASSIFICATION: SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

X-KEYSCORE C2C Session Viewer

Session 15 of 17

Date/Time	Case Notation	From IP	To IP	From Port	To Port	Protocol	Length
2011-04-11 13:47:44	3-411846/000000	192.██████████ (Private Address)	10.██████████ (Private Address)	4307	12468	ICP	774

Session Headers (3) Meta (7) Attachments (1)

Formatter: ASCII Send to: Download Session Mode: Snippet Options Search Content Enter text to search

Quick Clicks

- Session
- Attachments
 - unknown
 - lex
 - unknown_516.x-ww
- One-Click Searches
 - Find fingerprint
 - ndis/discovery/feur.s
 - http/getwith_content
 - ndis/discovery/feur.s
 - Find traffic on
 - 192.██████████
 - 10.██████████
 - Find application
 - http/get/x-www-form-urlencoded
 - Find proxy hash
 - 0d0c20f7
 - Find opposite side of sess
 - 192.██████████-4307C
 - 10.██████████

```

GET /?CAVIT HTTP/1.0
User-Agent: 62521C333F63DA79333FB2C02702E7BD2
Accept: */*
Host: 10.██████████:12468
Content-type: application/x-www-form-urlencoded
Connection: Keep-Alive

Reset from local:(1231) seq = 2661134980
  
```

This system is audited for USSID 18 and Human Rights Act compliance
CLASSIFICATION: SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Done

Notes:

- Strange User-Agent
- Probably NOT CNE but definitely something non-standard
- Content: maybe a HTTP tunnel for some weird protocol?
Reset from local...
- Should we write a Fingerprint?

SECRET//COMINT//REL TO USA, FVEY

SECRET//COMINT//REL TO USA, FVEY

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)

SECRET//COMINT//REL TO USA, FVEY

SECRET//COMINT//REL TO USA, FVEY

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

SECRET//COMINT//REL TO USA, FVEY

SECRET//COMINT//REL TO USA, FVEY



More about searches

- Many different searches
 - Base search is Full Log DNI
 - Depending on traffic type, will generate searchable results for (example):

HTTP Activity	Network Information	GEO Info
Extracted Files	Email Addresses	Registry
Logins and Passwords	Document Metadata	Machine Info

- workflow – a user query that is run automatically usually every 24 hours

SECRET//COMINT//REL TO USA, FVEY

XKEYSCORE Gotchas



- Not all sites run latest XKEYSCORE software or fingerprints
- fingerprint submission:
 - XKEYSCORE team weighs mission-worthiness of user fingerprints vs computational cost
- Content and metadata ageoff

SECRET//COMINT//REL TO USA, FVEY

TOP SECRET//COMINT//REL TO USA, FVEY

XKEYSCORE CNE



- Lots of endpoint data flows into XKS
TAO (no ECIs), GCHQ (almost all)
- Other limited flows include SIGINT
Forensics Center, TAO STAT
- XKEYSCORE works well for endpoint data
- Sometimes the paradigm breaks (e.g.
collected browser history file)

TOP SECRET//COMINT//REL TO USA, FVEY

TOP SECRET//COMINT//REL TO USA, FVEY

XKEYSCORE CNE (more)



- **Payload types:**
dirwalk, extracted file, system survey, network config, captured credentials, registry query, key logger, etc.
- **Labeled dnt_payload in appid/fingerprint ontology**
- **Let's look at some DANDERSPRITZ data...**

TOP SECRET//COMINT//REL TO USA, FVEY

TOP SECRET//COMINT//REL TO USA, FVEY

XKEYSCORE CNE (more)



XK Session Viewer - Mozilla Firefox

https://xks-central.compsa.af.mil:8443/XKEYSCORE/layouts/popOutLayout.jsp?pageTitle=Session+Viewer&showUrl=%2FXKEYSCORE%2F%2FmetaViewer!

This system is audited for US SID 18 and Human Rights Act compliance
 CLASSIFICATION: TOP SECRET//COMINT//REL TO USA, AUS, CAN, GDR, NZL

X-KEYSCORE C2C Session Viewer

Session: 50 of 703

Date/Time	Case Fixation	From IP	To IP	From Port	To Port	Protocol	Length
2011-04-12 02:06:12	CC.WYUJCCAACDTD						10074

Session: Header (3) Meta (4)

Format: XML_PAYLOAD Send to: Download Session Mode: Snippet Use one Search context: enter text to search Clear

Quick Clicks

- Security
- One-Click Searches
 - Find Intranet
 - ... exfil/experimental/process
 - Find traffic on
 - ... dnt_payload/processlist
 - Find opposite side of case on
 - ... C ->

PAYLOAD XML

```

<Process creationTime="2011-04-05T00:37:09.631250000" description="initia." pid="463" ppid="302">lsass.exe</Process>
<Process creationTime="2011-04-05T00:37:11.72343750000" description="initia." pid="655" ppid="140">svchost.exe</Process>
<Process creationTime="2011-04-05T00:37:34.781250000" description="initia." pid="728" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:37:35.359375000" description="initia." pid="792" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:37:36.484375000" description="initia." pid="844" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:37:40.703125000" description="initia." pid="863" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:37:41.390525000" description="initia." pid="895" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:37:42.718750000" description="initia." pid="968" ppid="140">ccsvchost.exe</Process>
<Process creationTime="2011-04-05T00:37:54.640525000" description="initia." pid="1348" ppid="440">msdtc.exe</Process>
<Process creationTime="2011-04-05T00:37:57.171875000" description="initia." pid="1454" ppid="440">fwrts.exe</Process>
<Process creationTime="2011-04-05T00:37:57.710750000" description="initia." pid="1530" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:37:58.046375000" description="initia." pid="1532" ppid="440">HLPlaserJetService.exe</Process>
<Process creationTime="2011-04-05T00:38:00.625000000" description="initia." pid="1530" ppid="440">HP5Svc.exe</Process>
<Process creationTime="2011-04-05T00:38:00.750000000" description="initia." pid="1630" ppid="140">KPMONJ-1.exe</Process>
<Process creationTime="2011-04-05T00:38:01.234375000" description="initia." pid="1620" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:38:01.421875000" description="initia." pid="1644" ppid="440">NHOSVCI.EXE</Process>
<Process creationTime="2011-04-05T00:38:02.125000000" description="initia." pid="1672" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:38:02.500000000" description="initia." pid="1696" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:38:02.625000000" description="initia." pid="1720" ppid="440">ftvscan.exe</Process>
<Process creationTime="2011-04-05T00:38:08.046375000" description="initia." pid="1802" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:38:10.437500000" description="initia." pid="1924" ppid="140">VMwareSvc.exe</Process>
<Process creationTime="2011-04-05T00:38:14.562500000" description="initia." pid="2216" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:38:14.671875000" description="initia." pid="2240" ppid="1644">NHSTMS2.FXFC</Process>
<Process creationTime="2011-04-05T00:38:17.625000000" description="initia." pid="2350" ppid="2240">NHSTMS2.FXFC</Process>
<Process creationTime="2011-04-05T00:38:23.031250000" description="initia." pid="2620" ppid="656">winbrvse.exe</Process>
<Process creationTime="2011-04-05T00:45:47.108340500" description="initia." pid="1638" ppid="704">explorer.exe</Process>
<Process creationTime="2011-04-05T00:45:48.072375000" description="initia." pid="1736" ppid="844">svchost.exe</Process>
<Process creationTime="2011-04-05T00:45:54.681250000" description="initia." pid="2042" ppid="1688">VMwareRay.exe</Process>
<Process creationTime="2011-04-05T00:45:57.839375000" description="initia." pid="2838" ppid="1688">VMwareUser.exe</Process>
<Process creationTime="2011-04-05T00:46:00.750750000" description="initia." pid="2956" ppid="1688">App.exe</Process>
<Process creationTime="2011-04-05T00:46:02.203303200" description="initia." pid="755" ppid="1000">ctfract.exe</Process>
<Process creationTime="2011-04-05T00:46:06.675359700" description="initia." pid="452" ppid="1000">hpsservice.exe</Process>
<Process creationTime="2011-04-05T00:46:15.408322600" description="initia." pid="3530" ppid="3395">cominc.exe</Process>
<Process creationTime="2011-04-05T00:46:25.535849300" description="initia." pid="328" ppid="1823">dwmn.exe</Process>
<Process creationTime="2011-04-05T00:56:53.997113900" description="initia." pid="4050" ppid="392">logon.scr</Process>
<Process creationTime="2011-04-11T22:28:03.260310500" description="Started" pid="2424" ppid="320">csrss.exe</Process>
<Process creationTime="2011-04-11T22:28:03.476595500" description="Started" pid="5130" ppid="320">svchost.exe</Process>
<Process creationTime="2011-04-11T22:25:30.503396000" description="Started" pid="5440" ppid="320">csrss.exe</Process>
<Process creationTime="2011-04-11T22:25:39.660251000" description="Started" pid="5430" ppid="320">winlogon.exe</Process>
<Process creationTime="2011-04-11T22:25:00.453250000" description="Started" pid="363" ppid="320">csrss.exe</Process>
<Process creationTime="2011-04-11T22:25:00.609140000" description="Started" pid="138" ppid="320">winlogon.exe</Process>
<Process creationTime="2011-04-11T22:48:36.768533500" description="Started" pid="4656" ppid="320">csrss.exe</Process>
<Process creationTime="2011-04-11T22:48:36.956375000" description="Started" pid="2572" ppid="320">svchost.exe</Process>

```

This system is audited for US SID 18 and Human Rights Act compliance
 CLASSIFICATION: TOP SECRET//COMINT//REL TO USA, AUS, CAN, GDR, NZL

Done

TOP SECRET//COMINT//REL TO USA, FVEY

TOP SECRET//COMINT//REL TO USA, FVEY

XKEYSCORE CNE (more)



- Recent Developments
 - Upgrade of XKEYSCORE CNE
 - Keyloggers: keylogger/perfect/extension
 - PCAP Reingestion
- Router Redirection

TOP SECRET//COMINT//REL TO USA, FVEY

TOP SECRET//COMINT//REL TO USA, FVEY

Counter CNE Methodology



(refer to Counter CNE Resources slide...)

- Hypothesis/research-driven
 - "Could South Korean CNE be using similar selectors to FVEY CNE?"
 - "What keywords could be used to find keyloggers ("example: keylog OR keystroke")"
- Bogus or Unusual Traffic
 - HTTP GET with content (example in this presentation)
 - HTTP POST at odd hours (from Russia 0200-0359Z)
 - Funky user agents
- Known-Host or User driven (e.g. drop sites)
- **XKEYSCORE is GOOD at these kinds of things**

TOP SECRET//COMINT//REL TO USA, FVEY

TOP SECRET//COMINT//REL TO USA, FVEY

CNE-Specific



- Registry searches (e.g. SIMBAR)
- Fused Active/Passive search
 - common selectors
 - document hashes
- Known Processes (malicious executables or code)
 - ... Let's enhance the process list appid
- map-reduce within CNE cluster using GENESIS calls

TOP SECRET//COMINT//REL TO USA, FVEY

TOP SECRET//COMINT//REL TO USA, FVEY

XKEYSCORE Doesn't Do...



- ... at all (well, automatically, anyways)
 - Paired traffic heuristic-based approach
 - HTTP[S] imbalance (e.g. GET without response)
 - IP/DNS mismatch*
- ... on an automatic basis
 - Network or host characterization
 - Changes in IP/DNS mapping over time
 - Changes over time in malware comms

TOP SECRET//COMINT//REL TO USA, FVEY

TOP SECRET//COMINT//REL TO USA, FVEY

Counter CNE Resources



- *How to Discover Intrusions [using XKEYSCORE]* by [REDACTED] and [REDACTED] (paper)
- MHS INDEX – Foreign CNE Discovery Page
https://wiki.itd.nsa/wiki/Foreign_CNE_Discovery
- CSEC and GCHQ – DONUT (unknown protocols):
<https://tiso.sigint.cse/snipehunt/index.php/DONUT>
- GCHQ Discovery Posted some Research of Detecting Man-on-the-Side Attacks:
<https://tiso.sigint.cse/snipehunt/index.php/MOTS>
- GCQH Disco Team posts POC's for different Intrusions and some Details:
<https://wiki.gchq/index.php/Discovery>
- The GCHQ DISCO team also posts Discovery Theories they run once a week:
https://wiki.gchq/index.php/Discovery_Afternoons
- XKEYSCORE Fingerprints

TOP SECRET//COMINT//REL TO USA, FVEY

TOP SECRET//COMINT//REL TO USA, FVEY

Success Story – MHS INDEX



Using TAO-obtained Iranian implant encryption keys, inline decrypt using XKS microplugin – IRGC-QF keylogger data!

The screenshot shows the XKS Session Viewer interface in Mozilla Firefox. The browser address bar displays the URL: https://xks-central.corp.nsa.ic.gov:8443/XKEYSCORE/layouts/popOutLayout.jsp?pageTitle=Session Viewer&rowUrl=%2FXKEYSCORE%2F%2Fmetaview. A red banner at the top states: 'This system is audited for USSID 18 and Human Rights Act compliance CLASSIFICATION: TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL'. Below this, the interface is titled 'X-KEYSCORE C2C Session Viewer'. A table shows session details for Session 15 of 70, with a datetime of 2011-03-28 19:51:28, case notation IRS1014, and communication between an IP from Iran (78.███) and an IP from the United States (174.███) on port 42325 to port 80 via TCP, with a length of 3203 bytes. The main display area shows the keylogger data for 'keylogger.txt' using a 'TXT' formatter. The data includes unread messages from Yahoo! Mail and a snippet of a page from http://us.mg4.mail.yahoo.com. A red circle highlights a redacted IP address in the keylogger output, with a red arrow pointing to the word 'Login' on the right side of the screen.

TOP SECRET//COMINT//REL TO USA, FVEY

TOP SECRET//COMINT//REL TO USA, FVEY

Points of Contact



- MHS Index Team

[REDACTED] : [REDACTED]@nsa.ic.gov

- CES/TRANGRESSION

[REDACTED] : [REDACTED]@nsa.ic.gov

[REDACTED] : [REDACTED]@nsa.ic.gov

- NSA/Countering Foreign Intelligence

[REDACTED] : [REDACTED]@nsa.ic.gov

- NTOC ??

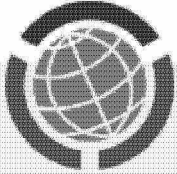
- XKEYSCORE

[REDACTED], [REDACTED] : xks-cne@r1.r.nsa

TOP SECRET//COMINT//REL TO USA, FVEY

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 31



WIKIMEDIA
META-WIKI

Content page

Discussion

Read

Edit

View history

Search Meta Go

Founding principles

Translate this page; This page contains changes which are not marked for translation.

Other languages:	العربية • مصرى • asturianu • беларуская (тарашкевіца) • български • català • čeština • Cymraeg • dansk • Deutsch • Zazaki • Ελληνικά • English • Esperanto • español • cuskara • فارسی • français • magyar • Bahasa Indonesia • italiano • 日本語 • 한국어 • Lëtzebuergesch • Baso Minangkabau • Bahasa Melayu • Nederlands • occitan • polski • پښتو • português • português do Brasil • русский • سنڌي • slovenčina • slovenščina • Basa Sunda • svenska • татарча/tatarça • українська • 中文

Wikimedia projects have certain **founding principles** in common. These principles may evolve or be refined over time, but they are considered ideals essential to the founding of the Wikimedia projects – not to be confused with the Wikimedia Foundation (which also arose from the Wikimedia projects). People who strongly disagree with them are nonetheless expected to either respect them while collaborating on the site or turn to another site. Those unable or unwilling sometimes end up leaving the project.

These principles include:

1. Neutral point of view (NPOV) as a guiding editorial principle.
2. The ability of almost anyone to edit (most) articles without registration.
3. The "wiki process" as the final decision-making mechanism for all content.
4. The creation of a welcoming and collegial editorial environment.
5. Free licensing of content; in practice defined by each project as public domain, GFDL, CC BY-SA or CC BY.
6. Maintaining room for fiat to help resolve particularly difficult problems. On a dozen projects, an Arbitration Committee has the authority to make certain binding, final decisions such as banning an editor.

Variants [edit]

Not all projects follow these principles in the same way.

- Some apply neutrality by allowing a plurality of items which are individually not neutral (Commons, which says "Commons is not Wikipedia, and files uploaded here do not necessarily need to comply with the Neutral point of view"), or have a simpler principle of 'being fair' (Wikivoyage, which says "Travel guides should *not* be written from a neutral point of view").
- Some allow non-wiki modes of collaboration and decision-making in some parts of their process (MediaWiki).
- Some allow limited use of fair-use media or other media that are not freely licensed.

- Main page
- Wikimedia News
- Translations
- Recent changes
- Random page
- Help
- Babel
- Community
- Wikimedia Resource Center
- Wikimedia Forum
- Mailing lists
- Requests
- Babylon
- Reports
- Research
- Planet Wikimedia
- Beyond the Web
- Meet Wikimedians
- Events
- Movement affiliates
- Donate
- Print/export
- Create a book
- Download as PDF
- Printable version

- Tools
- What links here
- Related changes
- Special pages
- Permanent link
- Page information
- Cite this page
- Link by ID
- In other languages
- Add links

See also [edit]

- [Wikimedia Foundation mission statement](#)
- [Wikimedia values](#) — The six values of the Wikimedia Foundation
- [In a nutshell, what is Wikipedia? And what is the Wikimedia Foundation? — The Wikimedia Foundation](#)

Categories: [Community](#) | [Global policies](#)

This page was last edited on 27 February 2018, at 07:58.

Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. See Terms of Use for details.

[Privacy policy](#) [About Meta](#) [Disclaimers](#) [Developers](#) [Cookie statement](#) [Mobile view](#)



Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 32

COMMUNITY WIKIPEDIA FOUNDATION TECHNOLOGY

SHARE f g+

COMMUNITY, GLOBAL, LEGAL, WIKIMEDIA

Opposing Mass Surveillance on the Internet

By Yana Welinder
May 9th, 2014

GET CONNECTED f g+ in

GET OUR EMAIL UPDATES

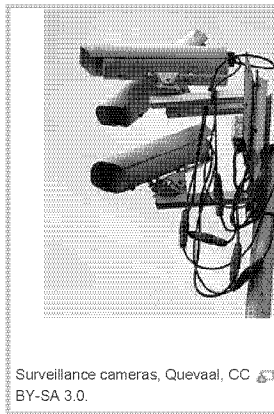
Your email address

Subscribe

Surveillance cameras, Quevaal, CC BY-SA 3.0. We are pleased to announce that the Wikimedia Foundation is signing the Necessary and Proportionate Principles on the application of human rights to surveillance. Privacy on the Internet is closely connected to our mission to disseminate free knowledge.[1] 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

We are pleased to announce that the Wikimedia Foundation is signing the Necessary and Proportionate Principles on the application of human rights to surveillance.

Privacy on the Internet is closely connected to our mission to disseminate free knowledge.[1] 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.

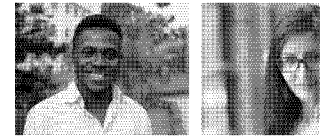


Surveillance cameras, Quevaal, CC BY-SA 3.0.

Although the recent conversation about internet surveillance was spurred by the revelation of a US government program, PRISM, a report issued by the United Nations Special Rapporteur on the Freedom of Opinion and Expression makes it clear that surveillance by governments is global, ubiquitous, and generally unchecked. The Necessary and Proportionate Principles are intended to provide a framework for human rights laws to address modern surveillance technologies.[2] They demand that governments respect international law and human rights by complying with basic principles such as:

- **Proportionality:** Surveillance of communications is highly intrusive and implicates privacy rights and freedom of expression. This should be carefully weighed against any benefit sought to be achieved.
- **User Notification:** Individuals need to know if they will be the subject of surveillance and have enough time and information to appeal the decision.
- **Transparency:** Countries must be transparent about the extent of surveillance and the techniques employed.

MEET OUR COMMUNITY



The one-man band Nigerian cinema into Wikipedia *Wikipedia is a "plant and harvest" free knowledge: Ar Aghayan*

More Community Profiles

MOST VIEWED THIS MONTH

'Monumental' winners from th world's largest photo contest showcase history and heritage

The top fifteen images from Wiki...

Türkiye'den Vikipedi'ye erişim engeli halen devam ediyor

Vikipedi'nin tüm dil sürümleri, Nisan ayını

New monthly dataset shows w people fall into Wikipedia rabl holes

The Wikimedia Foundation's Analytics tea

ARCHIVES

FEBRUARY 2018

JANUARY 2018

• **Integrity of Communications and Systems:** Governments should not compel ISPs or hardware and software vendors to build monitoring capability into their systems.

DECEMBER 2017

NOVEMBER 2017

OCTOBER 2017

OLDER POSTS

26

The Necessary and Proportionate Principles project was led by several groups, including the Electronic Frontier Foundation, Access, and Privacy International. The principles were developed through a consultation with civil society groups and international experts in communications surveillance law, policy, and technology. So far, the Principles have been advocated by over 400 organizations and many individuals. The signatories include Wikimedia Mexico and several Wikimedians. Today, we are proud to join their efforts.

Yana Welinder

Legal Counsel, Wikimedia Foundation^[9]

1. † As we previously discussed, the Foundation believes that government surveillance can compromise our values of freedom of speech and access to information.
2. † For more information about the purpose of the Principles, see here.
3. † Special thanks to Roshni Patel, WMF Privacy Fellow, for her work on this blog post.

WORK AT WIKIMEDIA

Work with the foundation that supports W and its sister projects around the world. A and join us

5 Comments on Opposing Mass Surveillance on the Internet

Global Ceo 3 years

The people are massively supporting the uncensored internet and the founder of internet agrees with them. <http://globalceo.com/tim-berners-lee-web-should-be-basis-of-democracy/>

Share

Fae 4 years

Sorry, the links embedded in my last post do not seem to have been included. These were:

1. An email "Use of this list as evidence of consultation" to the Advocacy Advisors list http://lists.wikimedia.org/pipermail/advocacy_advisors/2014-May/thread.html
2. The discussion in 2013 by Wikimedia UK volunteers at https://wikimedia.org.uk/wiki/Water_cooler/2013#International_Principles_on_the_Application_of_Human_Rights_to_Communications_Surveillance

Share

Fae 4 years

Hi Roshni, thanks for your prompt response.

I was not aware of the Advocacy Advisors email list, members of that list are neither elected nor are Wikimedia groups such as Wikimedia LGBT asked to provide representation on the list. It is not evidence of community consultation. I have today joined the list and raised this question of scope at .

Your personal reading of the document does not agree with mine, or many other Wikimedians, the discussion in 2013 by Wikimedia UK volunteers at may be a helpful reference.

The list under "Legitimate Aim" uses wording that cannot be assumed to be defined by the preamble. Further, it is clear that in any country where LGBT activities were unlawful, any legally recognized organization would have no obligation to respect the private lives of LGBT minorities. The document appears to deliberately circumvent this issue by its careful choice of wording. As a relatively short set of principles, where other minority groups have been specifically listed for protection, yet LGBT or sexual orientation remains invisible, can only be a political convenience so that the principles do not break the law in countries where homosexuality is unlawful.

I am deeply disappointed that the community was not widely consulted so that this problem could not be properly discussed, before committing the Foundation to this flawed document.

Share

Roshni Patel 4 years

Hi Fae,

Prior to signing on to the Necessary and Proportionate Principles, we consulted the advocacy advisors. You can find that here.

The list of prohibited discriminations under the "Legitimate Aim" principle is non-exclusive and includes "other status." Given that sexual orientation was listed in the preamble, it would certainly be included under "other status".

Share

Fae 4 years

The document will be offensive to many, as LGBT minorities have been explicitly excluded from the "Legitimate Aim" section, despite "sexual orientation" being mentioned in the unenforceable preamble. As a consequence this policy supports any Government who wish to track LGBT minorities for any reason. In the light of countries recently attempting to make having a profile on Grindr a crime for its citizens, this is not a theoretical scenario.

Could someone please provide some links to the necessary community consultation in advance of this political action of the WMF?

Share

Comments are closed.

WIKIMEDIA FOUNDATION

The Wikimedia Foundation, Inc is a nonprofit charitable organization dedicated to encouraging the growth, development and distribution of free, multilingual content, and to providing the full content of these wiki-based projects to the public free of charge. [Get involved](#) | [Log in](#)

WIKIMEDIA PROJECTS

The Wikimedia Foundation operates some of the largest collaboratively edited reference projects in the world.

- WIKIPEDIA
- WIKIDATA
- WIKISPECIES
- COMMONS
- WIKINews
- WIKIVERSITY
- MEDIAWIKI
- WIKIQUOTE
- WIKIVOYAGE
- WIKIBOOKS
- WIKISOURCE
- WIKTIONARY

WIKIMEDIA MOVEMENT AFFILIATES

The Wikimedia projects have an international scope, and the Wikimedia movement he already made a significant impact throughout the world. To continue this success on a organizational level, Wikimedia is building an international network of associated organizations.

- WIKIMEDIA CHAPTERS
- THEMATIC ORGANIZATIONS
- WIKIMEDIA USER GROUPS

This work is licensed under a Creative Commons Attribution 3.0 unported license. Some images under CC BY-SA. [Read our Terms of Use and Privacy policy.](#) | Powered by [WordPress.com](#) VIP

u

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 33



Policy Action List

Join our mailing list to keep up with our policy initiatives.

Privacy

Everyone should be free to read and write without governments looking over their shoulders.



"What Are You Looking At?" by Jonas Bengtsson, licensed under CC BY 2.0 / cropped.

Why You Should Care

- 🐦 Privacy is essential for our intellectual freedom: reading, writing, and researching.
- 🐦 People should be free to read and write without fear of governments or advertisers looking over their shoulder.
- 🐦 Privacy can be an important personal preference even for those that have nothing to hide.

Privacy is the bedrock of intellectual freedom and thus of free knowledge. It sustains freedom of expression and association, which in turn enable inquiry, dialogue, and creation. Privacy is essential to Wikimedia's vision of empowering everyone to share in the sum of all human knowledge. People should not have to look over their shoulders before searching, pause before contributing to controversial articles, or refrain from sharing verifiable but unpopular information.

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.

People also need to feel comfortable that they can read Wikipedia without the fear that the government or other third parties are tracking or watching them. Therefore, all traffic to and from the Wikimedia projects is encrypted through the HTTPS protocol. We also use Strict Transport Security (HSTS), which instructs web browsers to only interact with Wikimedia projects over an encrypted connection, protecting against efforts to break HTTPS and intercept traffic.

Your Help is Welcome

To discuss or help translate this page visit the public policy discussion group.

Wikimedia projects are not built in isolation. The privacy practices of other sites with reliable sources impact the Wikimedia mission to collect and share knowledge. For our free knowledge projects to work, we need security and privacy across the internet so editors and readers can freely research the sources needed to build Wikipedia.

In particular, internet users cannot be subjected to mass surveillance, which chills intellectual curiosity and creativity. Privacy is a fundamental right recognised under international law like the International Covenant on Civil and Political Rights (Article 17) and the Universal Declaration of Human Rights (Article 12). Indiscriminate mass surveillance violates this fundamental right. We strongly oppose mass surveillance by any government or entity. To that end, we signed the Necessary and Proportionate Principles on the application of human rights to surveillance that demand that governments respect basic principles such as:

- Proportionality: The need for surveillance should be carefully weighed against the implications for privacy rights and freedom of expression.
- User Notification: Individuals who will be the subject of surveillance must have enough time and information to appeal the decision.

- Transparency: Governments must be transparent about the extent of surveillance and the techniques they employ.
- Integrity of communication and systems: Governments should not compel internet service providers of hardware and software vendors to build monitoring capability into their systems.

In a time when the collection of private data has become a business model, Wikimedians believe in the importance of privacy. This human right protects our users and consequently the creation of free knowledge.

Related Resources

Global surveillance disclosures (2013–present)

Privacy by Design

Necessary and Proportionate

To discuss or help translate this page visit the public policy discussion group.

Keep up-to-date with Wikimedia's policy initiatives

JOIN

The list admins will not give your email address to others.



Wikimedia Public Policy

*Learn more about the
Wikimedia Foundation.*

Privacy Policy | About

Our Topics

Access

Copyright

Censorship

Intermediary Liability

Privacy

*Wikipedia® and other Wikimedia project names and logos are registered trademarks of the
Wikimedia Foundation, a non-profit organization.*

Text licensed under Creative Commons Attribution-ShareAlike 3.0 unported. Images are freely licensed with attribution.

Powered by WordPress.com VIP

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 34

WIKIPEDIA

Wikipedia:Sock puppetry



This page documents an English Wikipedia policy.

It describes a widely accepted standard that all editors should normally follow. Changes made to it should reflect consensus.



This page in a nutshell: The general rule is **one editor, one account**. Do not use multiple accounts to mislead, deceive, vandalize or disrupt; to create the illusion of greater support for a position; to stir up controversy; or to circumvent a block, ban, or sanction. Do not ask your friends to create accounts to support you. Do not revive old unused accounts and use them as different users, or use another person's account. Do not log out just to vandalize as an IP address editor.

Editors are generally expected to edit using at most one account. This improves accountability and increases community trust. While there are some valid reasons for maintaining multiple accounts, improper uses of multiple accounts (called **sock puppetry**, or **socking**) include attempts to deceive or mislead other editors, disrupt discussions, distort consensus, avoid sanctions, evade blocks, or otherwise violate community standards and policies.

Sock puppetry takes various forms:

- Logging out to make problematic edits as an IP address
- Creating new accounts to avoid detection
- Using another person's account (piggybacking)
- Reviving old unused accounts (sometimes referred to as sleepers) and presenting them as different users
- Persuading friends or colleagues to create accounts for the purpose of supporting one side of a dispute (usually called meatpuppetry)

Misuse of multiple accounts is a serious breach of community trust. It may lead to:

- a block of all affected accounts
- a ban of the user (the *sockmaster* or *sockpuppeteer*) behind the accounts (each of which is a *sockpuppet* or *sock*)
- on-project exposure of all accounts and IP addresses used across Wikipedia and its sister projects
- the (potential) public exposure of any "real-world" activities or personal information deemed relevant to preventing future sock puppetry or certain other abuses.^[1]



The origin of the term "sock puppet" is a type of toy puppet.

Conduct policies

Aspersions

Block evasion

Civility

Clean start

Consensus

Dispute resolution

Edit warring

Editing policy

Harassment

Non-discrimination policy

No personal attacks

JA3274

An editor using multiple accounts for *valid* reasons should, on each account's user page, list all the other accounts with an explanation of their purpose (see below). Optionally, the user and user talk pages of some of the accounts can be redirected to those of another. Editors who use unlinked alternative accounts, or who edit as an IP address editor separate from their account, should carefully avoid any crossover on articles or topics because even innocuous activities such as copy editing, wikifying, or linking might be considered sock puppetry in some cases and innocuous intentions will not usually serve as an excuse.

<u>Ownership of content</u>
<u>Sock puppetry</u>
<u>Username policy</u>
<u>Vandalism</u>

Contents

Inappropriate uses of alternative accounts

Legitimate uses

Editing while logged out

Alternative account notification

Meatpuppetry

Sharing an IP address

Handling suspected sock puppets

Sockpuppet investigations

CheckUser

Blocking

Tagging

Proving you are not a sock

List of role accounts

See also

Guidelines

Essays

References

External links

Inappropriate uses of alternative accounts

Editors must not use alternative accounts to mislead, deceive, disrupt, or undermine consensus. This includes, but is not limited to:

- **Creating an illusion of support:** Alternative accounts must not be used to give the impression of more support for a position than actually exists.
- **Editing project space:** Undisclosed alternative accounts are not to be used in discussions internal to the project.^[2]

- **Circumventing policies:** Policies apply per person, not per account. Policies such as the three-revert rule are for each person's edits. Using a second account to violate policy will cause any penalties to be applied to your main account.
- **Strawman socks:** Creating a separate account to argue one side of an issue in a deliberately irrational or offensive fashion, to sway opinion to another side.
- **Evasion of sanctions:** Sanctions apply to individual editors, not to accounts. Using a second account to edit in violation of an active block or community sanction will result in further sanctions, which may include removal of your contributions. See also WP:EVASION.
- **Contributing to the same page or discussion with multiple accounts:** Editors may not use more than one account to contribute to the same page or discussion in a way that suggests they are multiple people. Contributing to the same page with clearly linked, legitimate, alternative accounts (e.g. editing the same page with your main and public computer account or editing a page using your main account that your bot account edited) is not forbidden.
- **Avoiding scrutiny:** Using alternative accounts that are not fully and openly disclosed to split your editing history means that other editors may not be able to detect patterns in your contributions. While this is permitted in certain circumstances (see legitimate uses), it is a violation of this policy to create alternative accounts to confuse or deceive editors who may have a legitimate interest in reviewing your contributions.
- **"Good hand" and "bad hand" accounts:** Using one account for constructive contributions and the other one for disruptive editing or vandalism.
- **Editing while logged out in order to mislead:** Editing under multiple IP addresses may be treated as the same level of disruption as editing under multiple accounts when it is done deceptively or otherwise violates the principles of this policy. When editors log out by mistake, they may wish to contact an editor with oversight access to ensure there is no misunderstanding.
- **Misusing a clean start** by switching accounts or concealing a clean start in a way that avoids scrutiny is considered a breach of this policy; see Wikipedia:Clean start.
- **Role accounts:** Because an account represents your edits as *an individual*, "role accounts", or accounts shared by multiple people, are as a rule forbidden and blocked. Many first time editors may sign up an account with a username that implies it is a role account or is being shared. Such accounts are permitted only if the account information is forever limited to one individual; however, policy recommends that usernames avoid being misleading or disruptive. As such, if you edit for an organization, please refer to Wikipedia's username policy for guidance on choosing a name or a replacement name that can avoid these problems. Role account exceptions can be made for *non-editing* accounts approved to provide email access, accounts approved by the Wikimedia Foundation (list below), and approved bots with multiple managers. See Username policy – Sharing accounts.
- **Deceptively seeking positions of community trust.** You may not run for positions of trust without disclosing that you have previously edited under another account. Adminship reflects the community's trust in an individual, not an account, so when applying for adminship, it is expected that you will disclose past accounts openly, or email the arbitration committee if the accounts must be kept private. Administrators who fail to disclose past accounts risk being desysopped, particularly if knowledge of them would have influenced the outcome of the RfA.
- **Using more than one administrator account:** Editors may **not** have more than one account with administrator user rights, except for bots with administrator privileges. However, Foundation staff may operate more than one admin account, though they must make known who they are. If an administrator leaves the project, returns under a new username, and is nominated for adminship, he or she must resign or give up the administrator access of their old account.
- **Posing as a neutral or uninvolved commentator:** Using an alternative account to participate in a discussion about another account operated by the same person.

Legitimate uses

See also: the categories Wikipedians with alternative accounts and Wikipedia alternative accounts.

Alternative accounts have legitimate uses. For example, editors who contribute using their real name may wish to use a pseudonym for contributions with which they do not want their real name to be associated, or long-term users might create a new account to better understand the editing experience from a new user's perspective. These accounts are not considered sockpuppets. If you use a legitimate alternative account, it is your responsibility to ensure that you do not use it in an illegitimate manner according to this policy.

Valid reasons for an alternative account include:

- **Security:** You may register an alternative account for use when accessing Wikipedia through a public computer, connecting to an unsecured network, or other scenarios when there's a risk of your account being compromised. Such accounts should be publicly connected to the main account or use an easily identified name. For example, User:Mickey might use User:Mickey (alt) or User:Mouse, and redirect that account's user and talk pages to their main account.
- **Privacy:** A person editing an article which is highly controversial within his/her family, social or professional circle, and whose Wikipedia identity is known within that circle, or traceable to their real-world identity, may wish to use an alternative account to avoid real-world consequences from their editing or other Wikipedia actions in that area. Although a privacy-based alternative account is not publicly connected to your main account, it should not be used in ways outlined in the inappropriate uses section of this page, and if it is, the account may be publicly linked to your main account for sanctions. If you are considering using an alternative account under this provision, please read the notification section below.
- **Doppelgänger accounts:** A doppelgänger account is an account created with a username similar to your main account to prevent impersonation. Such accounts should not be used for editing. Doppelgänger accounts may be marked with the `{{doppelganger}}` or `{{doppelganger-other}}` tag, or can simply redirect to the main account's userpage.
- **Clean start under a new name:** A clean start is when a user stops using an old account in order to start afresh with a new account, usually due to past mistakes or to avoid harassment. A clean start is permitted only if there are no active bans, blocks, or sanctions in place against the old account. Do not use your new account to return to topic areas, disputes, editing patterns, or behaviors previously identified as problematic, and you should be careful not to do anything that looks like an attempt to evade scrutiny. A clean start requires that you no longer use your old account(s), which should note on their user pages that they are inactive—for example, with the `{{retired}}` tag—to prevent the switch being seen as an attempt to sock puppet.
- **Username violations:** If you are blocked for having an inappropriate username, and that is the sole reason for the block, you are permitted to create a new account with an appropriate username.
- **Compromised accounts:** If you are unable to access your account because you have lost the password or because someone has obtained or guessed your password, you may create a new account with a clean password. In such a case, you should post a note on the user page of each account indicating that they are alternative accounts for the same person. If necessary, you should also ask for an admin to block the compromised account. You may want to consider using a committed identity in advance to help deal with this rare situation should it arise later.
- **Humor accounts:** The community has accepted some obviously humorous alternate accounts, for example User:Bishzilla, User:Bishopod, User:Darwinbish, User:Darwinfish, User:Floquenstein's monster, and sometimes Lady Catherine Rollbacker-de Burgh (the Late).
- **Technical reasons:**
 - **Maintenance:** An editor might use an alternative account to carry out maintenance tasks, or to segregate functions so as to maintain a user talk page dedicated to the purpose. The second account should be clearly linked to the main account.
 - **Bots:** Bots are programs that edit automatically or semi-automatically. Editors who use bots are encouraged to create separate accounts, and ask that they be marked as bot accounts via

Wikipedia:Bots/Requests for approval, so that the automated edits can be filtered out of recent changes. Bots should be clearly linked to their owner's account. See Wikipedia:Bot policy.

- **Testing and training:** Users who use a lot of scripts and other tools may wish to keep a second, "vanilla" account, for testing how things appear to others; or for demonstrating Wikipedia's default appearance when training new users. The second account should be clearly linked to the main account, except where doing so would interfere with testing or training, e.g. creating an account named "user:example" to serve as an example account analogous to the website example.com.
- **Designated roles:** Editors with specific roles, such as Wikipedian in residence or Wikimedia Foundation employees, may have specific accounts for those roles. Note the account still belongs to an individual, not the role itself, and should be named as such. For example, User:ExampleName (WIR for Foo Museum) is an acceptable alternative account, but User:Wikipedian-in-residence for Foo Museum is not, because it is named after the role. It is not required that the names match, e.g. the main account User:JohnDoe could have the role account User:ExampleName (WIR for Foo Museum), but the accounts should be clearly connected. If the editor leaves the role, their role account must no longer be used. If a new editor assumes the role, they must create a new account.
- **Teaching:** Teachers who incorporate Wikipedia into their classes may create an account for the purpose of supervising students. Use of the account should be limited to articles and other pages directly related to students and classwork.

Alternative accounts should always be identified as such on their user pages, except where doing so would defeat the point of the account. Templates such as {{User alternative account}} or one of a selection of user boxes may be used for this purpose.

Editing while logged out

See also: Help:Logging in § Editing while logged out

There is no policy against editing while logged out *per se*. This happens for many reasons, including not noticing that the login session had expired, changing computers, going to a Wikipedia page directly from a link, and forgetting passwords. Editors who are not logged in must not actively try to deceive other editors, such as by directly saying that they do not have an account or by using the session for the inappropriate uses of alternate accounts listed earlier in this policy. To protect their privacy, editors who have edited while logged out are never required to connect their usernames to their IP addresses on-wiki.

If you have concerns that an IP editor is actually a user with an account who is editing while logged out in a way that is inappropriate, you can give the IP editor notice of this policy (template for notification), and if the behavior continues, you should contact a CheckUser privately and present the evidence to them.

Alternative account notification

See also: Wikipedia:Userboxes/Wikipedia/Related accounts

Except when doing so would defeat the purpose of having a legitimate alternative account, editors using alternative accounts should provide links between the accounts. Links should ideally take the form of all three of the following:

1. Similarities in the username (for example, User:Example might have User:Example public or User:Example bot).^[3]
2. Links on both the main and alternative account user pages, either informally or using the userbox templates made for the purpose. To link an alternative account to a main account, use the **main** account to tag any secondary accounts with {{User alternate acct | main account}} (using the main account shows


it's genuine) or `{{Public user}}` if the account is being used to maintain security on public computers. The main account may be marked with `{{User alternative account name|OtherName|...|OtherName[n]}}` or `{{User Alt Acct Master}}`.

3. Links in the alternative account signature: if not linking to both the alternative and main account, link to the alternative account, and if necessary provide a note there requesting contact be made via the main account, or simply redirect the user talk page.

Editors who have multiple accounts for privacy reasons should *consider* notifying a checkuser or members of the arbitration committee if they believe editing will attract scrutiny. Editors who heavily edit controversial material, those who maintain single purpose accounts, as well as editors considering becoming an administrator are among the groups of editors who attract scrutiny even if their editing behavior itself is not problematic or only marginally so. Concerned editors may wish to email the arbitration committee or any individual with checkuser rights (<https://en.wikipedia.org/w/index.php?title=Special%3AListUsers&group=checkuser>). Editors who have abandoned an account and are editing under a new identity are required to comply with the clean start policy.

Meatpuppetry

See also: Wikipedia:Canvassing



This section in a nutshell: Do not recruit your friends, family members, or communities of people who agree with you for the purpose of coming to Wikipedia and supporting your side of a debate. If you feel that a debate is ignoring your voice, remain civil, and seek comments from other Wikipedians or pursue dispute resolution. These are well-tested processes, designed to avoid the problem of exchanging bias in one direction for bias in another.

High-profile disputes on Wikipedia often bring new editors to the site. Some individuals may promote their causes by bringing like-minded editors into the dispute. These editors are sometimes referred to as meatpuppets, following a common Internet usage. While Wikipedia assumes good faith, especially for new users, recruiting new editors to influence decisions on Wikipedia is prohibited. A new user who engages in the same behavior as another user in the same context, and who appears to be editing Wikipedia solely for that purpose, may be subject to the remedies applied to the user whose behavior they are joining. Sanctions have been applied to editors of longer standing who have not, in the opinion of Wikipedia's administrative bodies, consistently exercised independent judgment.

Wikipedia has processes in place to mitigate the disruption caused by an influx of single-purpose editors:

- Consensus in many debates and discussions should ideally **not** be based upon number of votes, but upon policy-related points made by editors.
- In votes or vote-like discussions, new users may be disregarded or given significantly less weight, especially if there are many of them expressing the same opinion. Their comments may be tagged with a note pointing out that they have made few or no other edits outside of the discussion.
- A 2005 Arbitration Committee decision established that "for the purpose of dispute resolution when there is uncertainty whether a party is one user with sockpuppets or several users with similar editing habits they may be treated as one user with sockpuppets."^[4]

The term *meatpuppet* may be seen by some as derogatory and should be used with care, in keeping with Wikipedia's civility policy. Because of the processes above, it may be counterproductive to directly accuse someone of being a "meatpuppet", and doing so will often only inflame the dispute.

Sharing an IP address

"WP:SHARE" redirects here. For the policy prohibiting the sharing of accounts, see Wikipedia:Username policy § Sharing accounts. For the sharebox script, see User:TheDJ/Sharebox.

If two or more registered editors use the same computer or network connection, their accounts may be linked by a CheckUser. Editors in this position are advised to declare such connections on their user pages to avoid accusations of sockpuppetry. There are userboxes available for this; see {{User shared IP address}}.

Closely connected users may be considered a single user for Wikipedia's purposes if they edit with the same objectives. When editing the same articles, participating in the same community discussion, or supporting each other in any sort of dispute, closely related accounts should disclose the connection and observe relevant policies such as edit warring as if they were a single account. If they do not wish to disclose the connection, they should avoid editing in the same areas, particularly on controversial topics.

Handling suspected sock puppets

Sockpuppet investigations

Wikipedia:Signs of sock puppetry lists some of the signs that an account may be a sock puppet. If you believe someone is using sock puppets or meat puppets, you should create a report at Wikipedia:Sockpuppet investigations. In reporting suspected sock puppetry, you must obey the rules of WP:OUTING with regard to disclosure of personal or identifying information. Only blocked accounts should be tagged as Category:Suspected Wikipedia sockpuppets and only upon sufficient evidence that would stand up to scrutiny.

CheckUser

Further information:
Wikipedia:CheckUser

Editors with access to the CheckUser tool may consult the server log to see which IP addresses are linked to which accounts. CheckUser cannot confirm with certainty that two accounts are not connected; it

Sockpuppet investigations

Current cases

Sock puppetry policy

Information pages

Guide to filing cases

Administrator instructions

Signs of sock puppetry

SPI clerk pages

List of clerks

Noticeboard (archive 1, archive 2, archive 3)

Procedures

Training

SPI archives

Archived cases (historical)

Malformed Cases (whitelist)

can only show whether there is a technical link at the time of the check. In accordance with the Wikimedia Foundation's Privacy and Checkuser policies, checks are only conducted with good cause, and (subject to the exceptions in those policies) results are reported in such a way as to avoid or minimize disclosure of personal identifying information. Particularly, "fishing"—the use of CheckUser without good cause specific to a given user account—is prohibited.

Blocking

Further information: Wikipedia:Blocking policy


If a person is found to be using a sock puppet, the sock puppet account(s) should be blocked indefinitely. The main account may be blocked at the discretion of any uninvolved administrator. IP addresses used for sock puppetry may be blocked, but are subject to certain restrictions for indefinite blocks.

Tagging

Further information: Wikipedia:Sockpuppet investigations/SPI/Administrators instructions § Blocking and tagging

Proving you are not a sock

One possibility to prove that your account is not a sock puppet is the **Personal acquaintances** WikiProject. This project was started in 2008 in the German language Wikipedia and uses a WMF labs tool

Babel user information	
	<p>This is a <u>confirmed</u> (https://tools.wmflabs.org/pb/index.py?p=users&) main account and not a sock puppet. (→ <u>Verify</u> (https://tools.wmflabs.org/pb/index.py?p=user&name=Sock%20puppetry) - <u>info</u>)</p> <p>→ I have met this user, verify! (https://de.wikipedia.org/wiki/Wikipedia:Pers%C3%B6nliche_Bekanntschaften/neue_Anfragen?preset_user=Sock+puppetry&preset_comment=&uselang=en)</p>
Users by language	

(<https://tools.wmflabs.org/pb/beta/>) where users can confirm that they have met a real person operating one specific Wikipedia or Wikimedia account at a meetup in real life. The project and its tool meanwhile have been translated to several other languages and can be accessed with any account using the global single user login. Once you have registered as a participant (https://de.wikipedia.org/wiki/Wikipedia:Pers%C3%B6nliche_Bekanntschaften/neue_Anfragen?uselang=en) of *Personal acquaintances*, you need to be confirmed by three other participants in good standing before you can start confirming other real life persons yourself. For further information go to the project page linked above. You can show other Wikipedians that you are a real person by displaying the userbox `{{Template:User Personal acquaintances}}` on your userpage or the link to your list of confirmations via the url "https://tools.wmflabs.org/pb/beta/user/name/your_username/".

List of role accounts

- *Non-editing accounts that provide an easy way to contact internal email lists:*
 - [User:Arbitration Committee](#)
 - [User:Ban Appeals Subcommittee](#)
 - [User:Bureaucrats](#)
 - [User:Emergency](#)
 - [User:Mediation Committee](#)^[5]
 - [User:Oversight](#)
 - [User:Wikipedia Information Team](#)
 - [User:Accounts-enwiki-l](#)
- *Accounts approved by the Foundation:*

[Category:Wikipedia contact role accounts](#)

See also

- [smurf account](#)
- [Sockpuppet \(Internet\)](#)
- [Wikipedia:Sleeper accounts](#)
- [Wikipedia:Sockpuppet investigations](#)

Guidelines

- [Wikipedia:Canvassing](#)

Essays

- [Wikipedia:Anything to declare?](#)
- [Wikipedia:Cabals](#)
- [Wikipedia:Consequences of sock puppetry](#)
- [Wikipedia:Don't be quick to assume that someone is a sockpuppet](#)
- [Wikipedia:Griefing](#)
- [Wikipedia:Lurkers](#)
- [Wikipedia:On privacy, confidentiality and discretion](#)
- [Wikipedia:Signs of sock puppetry](#)
- [Wikipedia:Single-purpose account](#)
- [Wikipedia:Tag team](#)
- [Wikipedia:The duck test](#)

References

1. [Wikimedia Foundation privacy policy](#):

"We hope that this never comes up, but we may disclose your personal information if we believe that it's reasonably necessary [...] to protect our organization, employees, contractors, users, or the public. We may also disclose your personal information if we reasonably believe it necessary to detect, prevent, or otherwise assess and address potential spam, malware, fraud, abuse, unlawful activity, and security or technical concerns."

Information under this policy is not gratuitously released, but may be made public at times in the context of detecting, confirming, preventing, and resolving issues related to actual or possible abuse.

2. See [Wikipedia:Requests for arbitration/Privateusings#Sockpuppetry](#).
3. Dissimilar names may cause confusion and create an impression of avoiding transparency; remember that the username appears in page histories even if you change the signature.
4. [Wikipedia:Requests for arbitration/Regarding Ted Kennedy#Sockpuppets](#)
5. Ownership of this account is passed between outgoing and newly-appointed Chairpersons, and the password is changed upon the transferral of ownership, so this is not a "role account".

External links

- [MeatBall:SockPuppet](#)

Wikipedia key policies and guidelines	
	<u>Five pillars</u> (What Wikipedia is not · <u>Ignore all rules</u>)
Content	✓ <u>Verifiability</u> · <u>No original research</u> · <u>Neutral point of view</u> · <u>What Wikipedia is not</u> · <u>Biographies of living persons</u> · <u>Image use</u> · <u>Wikipedia is not a dictionary</u> · <u>Article titles</u>
	✓ <u>Notability</u> · <u>Autobiography</u> · <u>Citing sources</u> · <u>Identifying reliable sources</u> (medicine) · <u>Do not include copies of primary sources</u> · <u>Plagiarism</u> · <u>Don't create hoaxes</u> · <u>Fringe theories</u> · <u>Patent nonsense</u> · <u>External links</u>
	✓ <u>Civility</u> · <u>Consensus</u> · <u>Editing policy</u> · <u>Harassment</u> · <u>Vandalism</u> · <u>Ignore all rules</u> · <u>No personal attacks</u> · <u>Ownership of content</u> · <u>Edit warring</u> · <u>Dispute resolution</u> · <u>Sock puppetry</u> · <u>No legal threats</u> · <u>Child protection</u> · <u>Paid-contribution disclosure</u>
Conduct	✓ <u>Assume good faith</u> · <u>Conflict of interest</u> · <u>Disruptive editing</u> · <u>Do not disrupt Wikipedia to illustrate a point</u> · <u>Etiquette</u> · <u>Gaming the system</u> · <u>Please do not bite the newcomers</u> · <u>Courtesy vanishing</u>
	✓ <u>Deletion policy</u> · <u>Proposed deletion</u> · <u>Criteria for speedy deletion</u> · <u>Attack page</u> · <u>Oversight</u> · <u>Proposed deletion of BLP</u> · <u>Proposed deletion (books)</u> · <u>Revision deletion</u>
Enforcement	✓ <u>Administrators</u> · <u>Banning</u> · <u>Blocking</u> · <u>Page protection</u>
Editing	✓

	Article size · Be bold · Disambiguation · Hatnotes · Set index articles · Subpages · User pages · Talk page guidelines (Signatures) · Broad-concept article · Project namespace (WikiProjects)
	Manual of Style (Contents) · Accessibility (Understandability) · Dates and numbers · Images · Layout · Lead section · Linking · Lists
	Classification · Categories, lists, and navigation templates · Categorization · Template namespace
WMF	✓ List of policies · Friendly space policy · Licensing and copyright · Privacy policy · Values · FAQ
	List of all policies and guidelines (✓ List of policies · ✓ List of guidelines) · Lists of attempts in creating fundamental principles

Sock puppetry

Guidance	Legitimate uses · Inappropriate uses · Meat puppetry · Canvassing · Username policy · Clean start · Single-purpose account · Sleeper accounts · Outing
Signs	Motivations · List of signs · Duck test · An obvious sock is obvious · Don't be quick to assume that someone is a sockpuppet · Lurkers
Investigations	Triggers · Administrators instructions · Requests for checkuser · CheckUser criteria
Consequences	Block · Ban

Wikipedia accounts and governance

Unregistered (IP) users	Why create an account? · Create an account · Request an account · IPs are human too · IP addresses are not people · IP hopper
Registered users	New account · Logging in (Reset passwords) · Username policy (Changing username · Usernames for administrator attention) · Unified login or SUL · Alternate account
Account security	Password strength requirements · User account security · Personal security practices · Two-factor authentication (Simple 2FA · 2FA for AWB) · Committed identity · On privacy, confidentiality and discretion · Compromised accounts
Blocks, global locks, bans, sanctions	Blocking policy (FAQ · Admins guide · Tools · Autoblock) · Appealing a block (Guide to appealing blocks · UTRS Unblock Ticket Request System) · Blocking IP addresses (Range blocks · IPv6 · Open proxies) · Global locks · Banning policy (ArbCom appeals) · Sanctions (Personal sanctions · General sanctions · Discretionary sanctions and Log · Essay) · Long-term abuse · Standard offer

Related to accounts	Sock puppetry · Single-purpose account · Sleeper account · Vandalism-only account · Wikibreak (Enforcer) · Retiring (Courtesy vanishing) · Clean start (Quiet return)
User groups and global user groups	Requests for permissions (Admin instructions · Admin guide) · Account creator (PERM) · Autopatrolled (PERM) · AutoWikiBrowser (PERM) · Confirmed (PERM) · Extended confirmed (PERM) · Edit filter helper · File mover (PERM) · Mass message sender (PERM) · New page reviewer (PERM) · Page mover (PERM) · Pending changes reviewer (PERM) · Rollback (PERM) · Template editor (PERM) · IP-block-exempt (Requests) · Courses access (Requests) · Bot accounts (Requests) · Global rights policy (OTRS Volunteer Response Team)
Advanced user groups	Administrators (RfA) · Bureaucrats (RfB) · Edit filter manager (Requests) · CheckUser and Oversight (Requests) · Founder
Committees and related	Arbitration Committee · Mediation Committee · Bot approvals group · Functionaries · Clerks
Governance	Administration (FAQ) · Formal organization · Editorial oversight and control · Quality control · Wikimedia Foundation (Board · Founder's seat · Meta-Wiki) · Leadership opportunities · WikiProjects · Elections · Policies and guidelines · Unbundling administrators' powers · Petitions · Noticeboards · Consensus · Dispute resolution · Reforms

Retrieved from "https://en.wikipedia.org/w/index.php?title=Wikipedia:Sock_puppetry&oldid=829183984"

This page was last edited on 7 March 2018, at 03:47.

Text is available under the [Creative Commons Attribution-ShareAlike License](#); additional terms may apply. By using this site, you agree to the [Terms of Use](#) and [Privacy Policy](#). Wikipedia® is a registered trademark of the [Wikimedia Foundation, Inc.](#), a non-profit organization.

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 35

Privacy policy

العربية azərbaycanca تۆرکجه български روچ کپتین بلوچی বাংলা bosanski català нохчийн
کوردی čeština català Cymraeg Deutsch Deutsch (Sie-Form) Zazaki Ελληνικά emiliàn
e rumagnòl English Canadian English British English Esperanto español euskara فارسی
suomi français Nordfriisk Frysk galego Avañe'ê עברית हिन्दी hrvatski magyar
Bahasa Indonesia italiano 日本語 ქართული ಕನ್ನಡ 한국어 Ripoarisch Кыргызча
Lëtzebuergesch Ligure lietuvių Basa Banyumasan македонски മലയാളം Bahasa
Melayu မြန်မာဘာသာ मازرونی Napulitano norsk bokmål नेपाली Nederlands nl-formal Diné
bizaad occitan ਪੰਜਾਬੀ Plautdietsch polski پښتو português português do Brasil română
русский Scots سنڌي පළා,ආ,ථ: සිංහල Soomaaliga shqip српски / srpski svenska
Kiswahili தமிழ் తెలుగు тоҷикӣ ไทย Türkçe удмурт українська اردو Tiếng Việt
მარგალური שׂד"י Yorùbá 粵語 中文 中文 (简体) 中文 (繁體)

This policy is approved by the Wikimedia Foundation Board of Trustees to apply to all [Wikimedia projects](#). It may not be circumvented, eroded, or ignored by local policies.

Want to help translate? [Translate the missing messages.](#)

This is a summary of the Privacy Policy. To read the full terms, [click here](#).

Disclaimer: This summary is not a part of the Privacy Policy and is not a legal document. It is simply a handy reference for understanding the full Privacy Policy. Think of it as the user-friendly interface to our Privacy Policy.

Because we believe that you shouldn't have to provide personal information to participate in the free knowledge movement, you may:

- Read, edit, or use any [Wikimedia Site](#) [without registering an account](#).
- Register for an account [without providing an email address or real name](#).

Because we want to understand how Wikimedia Sites are used so we can make them better for you, we collect some information when you:

- Make [public contributions](#).
- [Register an account](#) or update your user page.
- [Use the Wikimedia Sites](#).
- Send us [emails](#) or participate in a [survey](#) or [give feedback](#).

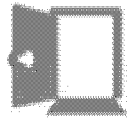
We are committed to:

- Describing how your information may be used or [shared](#) in this Privacy Policy.
- Using reasonable measures to keep your information [secure](#).
- Never [selling](#) your information or sharing it with third parties for marketing purposes.
- Only [sharing](#) your information in limited circumstances, such as to [improve the Wikimedia Sites](#), to [comply with the law](#), or to [protect you and others](#).

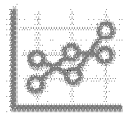
- Retaining your data for the shortest possible time that is consistent with maintaining, understanding, and improving the Wikimedia Sites, and our obligations under law.

Be aware:

- Any content you add or any change that you make to a Wikimedia Site will be publicly and permanently available.
- If you add content or make a change to a Wikimedia Site without logging in, that content or change will be publicly and permanently attributed to the IP address used at the time rather than a username.
- Our community of volunteer editors and contributors is a self-policing body. Certain administrators of the Wikimedia Sites, who are chosen by the community, use tools that grant them limited access to nonpublic information about recent contributions so they may protect the Wikimedia Sites and enforce policies.
- This Privacy Policy does not apply to all sites and services run by the Wikimedia Foundation, such as sites or services that have their own privacy policy (like the Wikimedia Shop (<https://shop.wikimedia.org>)) or sites or services run by third parties (like third-party developer projects on Wikimedia Cloud Services).
- As part of our commitment to education and research around the world, we occasionally release public information and aggregated or non-personal information to the general public through data dumps and data sets.
- For the protection of the Wikimedia Foundation and other users, if you do not agree with this Privacy Policy, you may not use the Wikimedia Sites.



[Introduction](#)



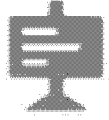
[Use of info](#)



[Sharing](#)

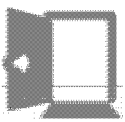


[Protection](#)



[Important info](#)

Contents [\[show\]](#)



Introduction

Welcome!

The Wikimedia Foundation is the nonprofit organization that operates collaborative, free knowledge websites, like

Wikipedia, Wikimedia
Commons, and
Wiktionary.

This Policy explains how we collect, use, and share your personal information.

- We collect very little personal information about you.
- We do not rent or sell your information to third parties.

By using Wikimedia Sites, you consent to this Policy.

The Wikimedia movement is founded on a simple, but powerful principle: we can do more together than any of us can do alone. We cannot work collectively without gathering, sharing, and analyzing information about our users as we seek new ways to make the Wikimedia Sites more useable, safer, and more beneficial.

We believe that information-gathering and use should go hand-in-hand with transparency. This Privacy Policy explains how the Wikimedia Foundation, the non-profit organization that hosts the Wikimedia Sites, like Wikipedia, collects, uses, and shares information we receive from you through your use of the Wikimedia Sites. It is essential to understand that, by using any of the Wikimedia Sites, you consent to the collection, transfer, processing, storage, disclosure, and use of your information as described in this Privacy Policy. That means that reading this Policy carefully is important.

We believe that you shouldn't have to provide personal information to participate in the free knowledge movement. You do not have to provide things like your real name, address, or date of birth to sign up for a standard account or contribute content to the Wikimedia Sites.

We do not sell or rent your nonpublic information, nor do we give it to others to sell you anything. We use it to figure out how to make the Wikimedia Sites more engaging and accessible, to see which ideas work, and to make learning and contributing more fun. Put simply: we use this information to make the Wikimedia Sites better for you.

After all, it's people like you, the champions of free knowledge, who make it

possible for the Wikimedia Sites to not only exist, but also grow and thrive.

Definitions

Because everyone (not just lawyers) should be able to easily understand how and why their information is collected and used, we use common language instead of more formal terms throughout this Policy. To help ensure your understanding of some particular key terms, here is a table of translations:

When we say...	... we mean:
"the Wikimedia Foundation" / "the Foundation" / "we" / "us" / "our"	The Wikimedia Foundation, Inc., the non-profit organization that operates the Wikimedia Sites.
"Wikimedia Sites" / "our services"	Wikimedia websites and services (regardless of language), including our main projects, such as Wikipedia and Wikimedia Commons, as well as mobile applications, APIs, emails, and notifications; excluding, however, sites and services listed in the "What This Privacy Policy Doesn't Cover" section below.
"you" / "your" / "me"	You, regardless of whether you are an individual, group, or organization, and regardless of whether you are using the Wikimedia Sites or our services on behalf of yourself or someone else.
"this Policy" / "this Privacy Policy"	This document, entitled the "Wikimedia Foundation Privacy Policy".
"contributions"	Content you add or changes you make to any Wikimedia Sites.
"personal information"	<p>Information you provide us or information we collect from you that could be used to personally identify you. To be clear, while we do not necessarily collect all of the following types of information, we consider at least the following to be "personal information" if it is otherwise nonpublic and can be used to identify you:</p> <ul style="list-style-type: none"> (a) your real name, address, phone number, email address, password, identification number on government-issued ID, IP address, user-agent information, credit card number; (b) when associated with one of the items in subsection (a), any sensitive data such as date of birth, gender, sexual orientation, racial or ethnic origins, marital or familial status, medical conditions or disabilities, political affiliation, and religion; and (c) any of the items in subsections (a) or (b) when associated with your user account.
"third party" / "third parties"	Individuals, entities, websites, services, products, and applications that are not controlled, managed, or operated by the Wikimedia Foundation. This includes other Wikimedia users and independent organizations or groups who help promote the Wikimedia movement such as <u>Wikimedia chapters</u> , <u>thematic organizations</u> , and <u>user groups</u> as well as <u>volunteers</u> , <u>employees</u> , <u>directors</u> , <u>officers</u> , <u>grant recipients</u> , and <u>contractors</u> of those organizations or groups.

We recognize that only a minority of you are familiar with technical terms like “tracking pixels” and “cookies” used in the Privacy Policy. Whether you are brand new to privacy terminology or you are an expert who just wants a refresher, you might find our [Glossary of Key Terms](#) helpful.

What This Privacy Policy Does & Doesn't Cover

Except as explained below, this Privacy Policy applies to our collection and handling of information about you that we receive as a result of your use of any of the Wikimedia Sites. This Policy also applies to information that we receive from our partners or other third parties. To understand more about what this Privacy Policy covers, please see below.

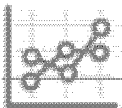
Examples of What This Privacy Policy Covers [\[Expand\]](#)

This Privacy Policy, however, does not cover some situations where we may gather or process information. For example, some uses may be covered by separate privacy policies (like those of the [Wikimedia Shop](#) (<https://store.wikimedia.org>)) or sites or services run by third parties (such as third-party developer projects on [Wikimedia Cloud Services](#)). To understand more about what this Privacy Policy does not cover, please see below.

More on what this Privacy Policy doesn't cover [\[Expand\]](#)

Where community policies govern information, such as the [CheckUser](#) policy, the relevant community may add to the rules and obligations set out in this Policy. However, they are not permitted to create new exceptions or otherwise reduce the protections offered by this Policy.

[Back to top](#) 



Use of info

Types of Information We Receive From You, How We Get It, & How We Use It

Your Public Contributions



Whatever you post on Wikimedia Sites can be seen and used by everyone.

The Wikimedia Sites were primarily created to help you share your knowledge with the world, and we share your contributions because you have asked us to do so.

When you make a contribution to any Wikimedia Site, including on user or discussion pages, you are creating a permanent, public record of every piece of content added, removed, or altered by you. The page history will show when your contribution or deletion was made, as well as your username (if you are signed in) or your IP address (if you are not signed in). We may use your public contributions, either aggregated with the public contributions of others or individually, to create new features or data-related products for you or to learn more about how the Wikimedia Sites are used.

Unless this Policy says otherwise, you should assume that information that you actively contribute to the Wikimedia Sites, including personal information, is publicly visible and can be found by search engines. Like most things on the Internet, anything you share may be copied and redistributed throughout the Internet by other people. Please do not contribute any information that you are uncomfortable making permanently public, like revealing your real name or location in your contributions.

You should be aware that specific data made public by you or aggregated data that is made public by us can be used by anyone for analysis and to infer information about users, such as which country a user is from, political affiliation, and gender.

[Back to top](#) 

Account Information & Registration

You do not need to create an account to use any Wikimedia Site.

If you do create an account, you do not need to give us your name or email address.

If you do not create an account, your contributions will be publicly attributed to your IP address.


Want to create an account? Great! Don't want to create an account? No problem!

You are not required to create an account to read or contribute to a Wikimedia Site, except under rare circumstances. However, if you contribute without signing in, your contribution will be publicly attributed to the IP address associated with your device.

If you want to create a standard account, in most cases we require only a username and a password. Your username will be publicly visible, so please be careful about using your real name as your username. Your password is only used to verify that the account is yours. Your IP address is also automatically submitted to us, and we record it temporarily to help prevent abuse. No other personal information is required: no name, no email address, no date of birth, no credit card information.

Once created, user accounts cannot be removed entirely (although you can usually hide the information on your user page if you choose to). This is because your public contributions must be associated with their author (you!). So make sure you pick a name that you will be comfortable with for years to come.

To gain a better understanding of the demographics of our users, to localize our services, and to learn how we can improve our services, we may ask you for more demographic information, such as gender or age, about yourself. We will tell you if such information is intended to be public or private, so that you can make an informed decision about whether you want to provide us with that information. Providing such information is always completely optional. If you don't want to, you don't have to—it's as simple as that.


[Back to top](#) 

Information Related to Your Use of the Wikimedia Sites

We may use common technologies to collect information about how you use Wikimedia Sites.

We use this information to enhance your user experience and to develop new features.

We want to make the Wikimedia Sites better for you by learning more about how you use them. Examples of this might include how often you visit the Wikimedia Sites, what you like, what you find helpful, how you get to the Wikimedia Sites, and whether you would use a helpful feature more if we explained it differently. We also want this Policy and our practices to reflect our community's values. For this reason, we keep information related to your use of the Wikimedia Sites confidential, except as provided in this Policy.

[Back to top](#) 


Information We Receive Automatically

Like other websites, we receive some information about you automatically when you visit the Wikimedia Sites. This information helps us administer the Wikimedia Sites and enhance your user experience.

Because of how browsers work and similar to other major websites, we receive some information automatically when you visit the Wikimedia Sites. This information includes the type of device you are using (possibly including unique device identification numbers, for some beta versions of our mobile applications), the type and version of your browser, your browser's language preference, the type and version of your device's operating system, in some cases the name of your internet service provider or mobile carrier, the website that referred you to the Wikimedia Sites, which pages you request and visit, and the date and time of each request you make to the Wikimedia Sites.

Put simply, we use this information to enhance your experience with Wikimedia Sites. For example, we use this information to administer the sites, provide greater security, and fight vandalism; optimize mobile applications, customize content and set language preferences, test features to see what works, and improve performance; understand how users interact

with the Wikimedia Sites, track and study use of various features, gain understanding about the demographics of the different Wikimedia Sites, and analyze trends.

[Back to top](#) 

Information We Collect

We use a variety of commonly-used technologies, like cookies, to understand how you use the Wikimedia Sites, make our services safer and easier to use, and to help create a better and more personalized experience for you.

We actively collect some types of information with a variety of commonly-used technologies. These generally include [tracking pixels](#), [JavaScript](#), and a variety of "locally stored data" technologies, such as [cookies](#) and [local storage](#). We realize that some of these technologies do not have the best reputation in town and can be used for less-than-noble purposes. So we want to be as clear as we can about why we use these methods and the type of information we collect with them.

Depending on which technology we use, locally stored data can be anything from text, pictures, and whole articles (as we explain further below) to personal information (like your [IP address](#)) and information about your use of the Wikimedia Sites (like your username or the time of your visit).

We use this information to make your experience with the Wikimedia Sites safer and better, to gain a greater understanding of user preferences and their interaction with the Wikimedia Sites, and to generally improve our services. We will never use third-party cookies, unless we get your permission to do so. If you ever come across a third-party data collection tool that has not been authorized by you (such as one that may have been mistakenly placed by another user or administrator), please report it to us at privacy@wikimedia.org (<mailto:privacy@wikimedia.org>).

Locally stored data, JavaScript, and tracking pixels help us do things like:

- Provide you with a personalized experience, such as using cookies to know your language preference, to remember the user preferences you


set so we can provide you with the customized look and feel that you want, and to tell you about interesting Wikimedia issues and events in your area.

- Deliver more relevant content to you faster. For example, we may use local storage to store your most recently read articles directly on your device, so they can be retrieved quickly. Also, we may use cookies to learn about the topics searched so that we can optimize the search results we deliver to you.
- Understand how you use the Wikimedia Sites, so that we know what works and what is useful. For example, we might use cookies to learn about the list of articles you are following on your watchlist so that we can recommend similar articles that you may be interested in.
- Understand how you use the Wikimedia Sites across different devices, so that we can make our varied Wikimedia Sites more efficient and effective for you.
- Make the Wikimedia Sites more convenient to use, such as by using cookies to maintain your session when you log in or to remember your username in the login field.

Want to know even more? You can read more about some of the specific cookies we use, when they expire, and what we use them for in our [FAQ](#).

We believe this data collection helps improve your user experience, but you may remove or disable some or all locally stored data through your browser settings, depending on your browser. You can learn more about some options you have in our [FAQ](#). While locally stored data may not be necessary to use our sites, some features may not function properly if you disable locally stored data.

While the examples above concerning information about you collected through the use of data collection tools are kept confidential in accordance with this Policy, please note that some information about the actions taken by your username is made publicly available through [public logs](#) alongside actions taken by other users. For example, a public log may include the date your account was created on a Wikimedia Site along with the dates that other accounts were created on a Wikimedia Site. Information available through public logs will not include personal information about you.

[Back to top](#) 

Emails

If you choose to provide your email address, we will keep it confidential, except as provided in this Policy.

We may occasionally send you emails about important information.

You may choose to opt out of certain kinds of notifications.


You have the option of providing an email address at the time of registration or in later interactions with the Wikimedia Sites. If you do so, your email address is kept confidential, except as provided in this Policy. We do not sell, rent, or use your email address to advertise third-party products or services to you.

We use your email address to let you know about things that are happening with the Foundation, the Wikimedia Sites, or the Wikimedia movement, such as telling you important information about your account, letting you know if something is changing about the Wikimedia Sites or policies, and alerting you when there has been a change to an article that you have decided to follow. Please note that if you email us, we may keep your message, email address, and any other information you provide us, so that we can process and respond to your request.

You can choose to limit some of these kinds of notifications, like those alerting you if an article changes. Others, such as those containing critical information that all users need to know to participate successfully in the Wikimedia Sites, you may not be able to opt out of. You can manage what kinds of notifications you receive and how often you receive them by going to your Notifications Preferences. You can learn more about email and notifications and how to change your preferences in our [FAQ](#).

We will never ask for your password by email (but may send you a temporary password via email if you have requested a password reset). If you ever receive such an email, please let us know by sending it to privacy@wikimedia.org (<mailto:privacy@wikimedia.org>), so we can investigate the source of the email.


Direct communications between users (such as messages sent through the "Email this user" feature), to the extent such communications are nonpublic and stored in or in transit through Wikimedia Foundation systems, are kept confidential by us, except as provided in this Policy.

[Back to top](#) 

Surveys & Feedback

We may ask you to provide us with information through a survey or provide feedback, but you will never be obligated to participate.

Participating in optional surveys or providing feedback helps us make the Wikimedia Sites better. Because every survey and request for feedback may be used for various purposes, we will tell you, at the time we give you the survey or request for feedback, how we plan on using your answers and any personal information you provide. If you don't feel comfortable with how we plan on using the survey or feedback results, you are not obligated to take the survey or give feedback.


[Back to top](#) 

Location Information

GPS & Other Location Technologies

If you consent, we can use commonly-used location technologies to show you more relevant content.

Some features we offer work better if we know what area you are in. But it's completely up to you whether or not you want us to use geolocation tools to make some features available to you. If you consent, we can use [GPS](#) (and other technologies commonly used to determine location) to show you more relevant content. We keep information obtained by these technologies confidential, except as provided in this Policy. You can learn more by checking out the list of examples of how we use these technologies in our [FAQ](#).


[Back to top](#) 

Metadata



We may automatically receive location data from your device. For example, if you upload a photo using the Wikimedia Commons mobile app, please be aware that the default setting on your mobile device typically results in the metadata associated with your photo being included in the upload.

Sometimes, we may automatically receive location data from your device. For example, if you want to upload a photo on the Wikimedia Commons mobile app, we may receive metadata, such as the place and time you took the photo, automatically from your device. Please be aware that, unlike location information collected using GPS signals described above, the default setting on your mobile device typically includes the metadata in your photo or video upload to the Wikimedia Sites. If you do not want metadata sent to us and made public at the time of your upload, please change your settings on your device.

[Back to top](#) 

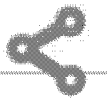
IP Addresses

When you visit any Wikimedia Site, we automatically receive the IP address of the device you are using to access the Internet, which can be used to infer your geographical location.

Finally, when you visit any Wikimedia Site, we automatically receive the IP address of the device (or your proxy server) you are using to access the Internet, which could be used to infer your geographical location. We keep IP addresses confidential, except as provided in this Policy. For example, if you make a contribution without signing into your account, your IP address used at the time will be publicly and permanently recorded. If you are visiting

Wikimedia Sites with your mobile device, we may use your IP address to provide anonymized or aggregated information to service providers regarding the volume of usage in certain areas. We use IP addresses for research and analytics; to better personalize content, notices, and settings for you; to fight spam, identity theft, malware, and other kinds of abuse; and to provide better mobile and other applications.

[Back to top](#) 




Sharing

When May We Share Your Information?

We may share your information when you give us specific permission to do so.

With Your Permission

We may share your information for a particular purpose, if you agree. You can find more information in the list of examples in our [FAQ](#).

[Back to top](#) 

For Legal Reasons


We will disclose your information in response to an official legal process only if we believe it to be legally valid. We will notify you of such requests when possible.

We may access, preserve, or disclose your personal information if we reasonably believe it necessary to satisfy a valid and legally enforceable warrant, subpoena, court order, law or regulation, or other judicial or administrative order. However, if we believe that a particular request for disclosure of a user's information is legally invalid or an abuse of the legal

system and the affected user does not intend to oppose the disclosure themselves, we will try our best to fight it. We are committed to notifying you via email at least ten (10) calendar days, when possible, before we disclose your personal information in response to a legal demand. However, we may only provide notice if we are not legally restrained from contacting you, there is no credible threat to life or limb that is created or increased by disclosing the request, and you have provided us with an email address.

Nothing in this Privacy Policy is intended to limit any legal objections or defenses you may have to a third party's request (whether it be civil, criminal, or governmental) to disclose your information. We recommend seeking the advice of legal counsel immediately if such a request is made involving you.


For more information, see our [Subpoena FAQ](#).

[Back to top](#) 

If the Organization is Transferred (Really Unlikely!)

In the unlikely event that the ownership of the Foundation changes, we will provide you 30 days notice before any personal information is transferred to the new owners or becomes subject to a different privacy policy.

In the extremely unlikely event that ownership of all or substantially all of the Foundation changes, or we go through a reorganization (such as a merger, consolidation, or acquisition), we will continue to keep your personal information confidential, except as provided in this Policy, and provide notice to you via the Wikimedia Sites and a notification on [WikimediaAnnounce-L](#) or similar mailing list at least thirty (30) calendar days before any personal information is transferred or becomes subject to a different privacy policy.

[Back to top](#) 

To Protect You, Ourselves & Others



We, or users with certain administrative rights, may disclose information that is reasonably necessary to:


- enforce or investigate potential violations of Foundation or community-based policies;
- protect our organization, infrastructure, employees, contractors, or the public; or
- prevent imminent or serious bodily harm or death to a person.

We, or particular users with certain administrative rights as described below, may need to share your personal information if it is reasonably believed to be necessary to enforce or investigate potential violations of our [Terms of Use](#), this Privacy Policy, or any Foundation or user community-based policies. We may also need to access and share information to investigate and defend ourselves against legal threats or actions.

Wikimedia Sites are collaborative, with users writing most of the policies and selecting from amongst themselves people to hold certain administrative rights. These rights may include access to limited amounts of otherwise nonpublic information about recent contributions and activity by other users. They use this access to help protect against vandalism and abuse, fight harassment of other users, and generally try to minimize disruptive behavior on the Wikimedia Sites. These various user-selected administrative groups have their own privacy and confidentiality guidelines, but all such groups are supposed to agree to follow our [Access to Nonpublic Information Policy](#). These user-selected administrative groups are accountable to other users through checks and balances: users are selected through a community-driven process and overseen by their peers through a logged history of their actions. However, the legal names of these users are not known to the Wikimedia Foundation.

We hope that this never comes up, but we may disclose your personal information if we believe that it's reasonably necessary to prevent imminent and serious bodily harm or death to a person, or to protect our organization, employees, contractors, users, or the public. We may also disclose your personal information if we reasonably believe it necessary to detect, prevent,


or otherwise assess and address potential spam, malware, fraud, abuse, unlawful activity, and security or technical concerns. (Check out the list of examples in our [FAQ](#) for more information.)

[Back to top](#) 

To Our Service Providers

We may disclose personal information to our third-party service providers or contractors to help run or improve the Wikimedia Sites and provide services in support of [our mission](#).

As hard as we may try, we can't do it all. So sometimes we use third-party service providers or contractors who help run or improve the Wikimedia Sites for you and other users. We may give access to your personal information to these providers or contractors as needed to perform their services for us or to use their tools and services. We put requirements, such as confidentiality agreements, in place to help ensure that these service providers treat your information consistently with, and no less protective of your privacy than, the principles of this Policy. (Check out the list of examples in our [FAQ](#).)

[Back to top](#) 

To Understand & Experiment

We may give volunteer developers and researchers access to systems that contain your information to allow them to protect, develop, and contribute to the Wikimedia Sites.

We may also share non-personal or aggregated information with third


parties interested in studying the Wikimedia Sites.

When we share information with third parties for these purposes, we put reasonable technical and contractual protections in place to protect your information consistent with this Policy.

The open-source software that powers the Wikimedia Sites depends on the contributions of volunteer software developers, who spend time writing and testing code to help it improve and evolve with our users' needs. To facilitate their work, we may give some developers limited access to systems that contain your personal information, but only as reasonably necessary for them to develop and contribute to the Wikimedia Sites.

Similarly, we may share non-personal or aggregated information with researchers, scholars, academics, and other interested third parties who wish to study the Wikimedia Sites. Sharing this information helps them understand usage, viewing, and demographics statistics and patterns. They then can share their findings with us and our users so that we can all better understand and improve the Wikimedia Sites.

When we give access to personal information to third-party developers or researchers, we put requirements, such as reasonable technical and contractual protections, in place to help ensure that these service providers treat your information consistently with the principles of this Policy and in accordance with our instructions. If these developers or researchers later publish their work or findings, we ask that they not disclose your personal information. Please note that, despite the obligations we impose on developers and researchers, we cannot guarantee that they will abide by our agreement, nor do we guarantee that we will regularly screen or audit their projects. (You can learn more about re-identification in our [FAQ](#).)

[Back to top](#) 

Because You Made It Public

Information that you post is public and can be seen and used by everyone.

Any information you post publicly on the Wikimedia Sites is just that – public. For example, if you put your mailing address on your talk page, that is public, and not protected by this Policy. And if you edit without registering or logging into your account, your IP address will be seen publicly. Please think carefully about your desired level of anonymity before you disclose personal information on your user page or elsewhere.

[Back to top](#) 




Protection

How Do We Protect Your Data?

We use a variety of physical and technical measures, policies, and procedures to help protect your information from unauthorized access, use, or disclosure.

We strive to protect your information from unauthorized access, use, or disclosure. We use a variety of physical and technical measures, policies, and procedures (such as access control procedures, network firewalls, and physical security) designed to protect our systems and your personal information. Unfortunately, there's no such thing as completely secure data transmission or storage, so we can't guarantee that our security will not be breached (by technical measures or through violation of our policies and procedures).

[Back to top](#) 

How Long Do We Keep Your Data?

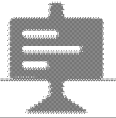


We only keep your personal information as long as necessary to maintain, understand, and improve the Wikimedia Sites or to comply with U.S. law.

Once we receive personal information from you, we keep it for the shortest possible time that is consistent with the maintenance, understanding, and improvement of the Wikimedia Sites, and our obligations under applicable U.S. law. Non-personal information may be retained indefinitely. (Check out the list of examples in our [FAQ](#).)

Please remember that certain information is retained and displayed indefinitely, such as your [IP address](#) (if you edit while not logged in) and any public contributions to the Wikimedia Sites.

[Back to top](#) 



Important info

For the protection of the Wikimedia Foundation and other users, if you do not agree with this Privacy Policy, you may not use the Wikimedia Sites.

Where is the Foundation & What Does That Mean for Me?

You are consenting to the use of your information in the U.S. and to the transfer of that information to other countries in connection to providing our services to you and others.

The Wikimedia Foundation is a non-profit organization based in San Francisco, California, with servers and data centers located in the U.S. If you decide to use Wikimedia Sites, whether from inside or outside of the U.S., you

consent to the collection, transfer, storage, processing, disclosure, and other uses of your information in the U.S. as described in this Privacy Policy. You also consent to the transfer of your information by us from the U.S. to other countries, which may have different or less stringent data protection laws than your country, in connection with providing services to you.

[Back to top](#) 

Our Response to Do Not Track (DNT) signals


We do not allow tracking by third-party websites you have not visited.

We do not share your data with third parties for marketing purposes.

We are strongly committed to not sharing nonpublic information with third parties. In particular, we do not allow tracking by third-party websites you have not visited (including analytics services, advertising networks, and social platforms), nor do we share your information with any third parties for marketing purposes. Under this Policy, we may share your information only under particular situations, which you can learn more about in the "[When May We Share Your Information](#)" section of this Privacy Policy.

Because we protect all users in this manner, we do not change our behavior in response to a web browser's "do not track" signal.

For more information regarding Do Not Track signals and how we handle them, please visit our [FAQ](#).

[Back to top](#) 

Changes to This Privacy Policy

Substantial changes to this Policy will not be made until after a public comment period of at least 30 days.

Because things naturally change over time and we want to ensure our Privacy Policy accurately reflects our practices and the law, it may be necessary to modify this Privacy Policy from time to time. We reserve the right to do so in the following manner:

- In the event of substantial changes, we will provide the proposed changes to our users in at least three (3) languages (selected at our discretion) for open comment period lasting at least thirty (30) calendar days. Prior to the start of any comment period, we will provide notice of such changes and the opportunity to comment via the Wikimedia Sites, and via a notification on [WikimediaAnnounce-L](#) or a similar mailing list.
- For minor changes, such as grammatical fixes, administrative or legal changes, or corrections of inaccurate statements, we will post the changes and, when possible, provide at least three (3) calendar days' prior notice via [WikimediaAnnounce-L](#) or similar mailing list.

We ask that you please review the most up-to-date version of our [Privacy Policy](#). Your continued use of the Wikimedia Sites after this Privacy Policy becomes effective constitutes acceptance of this Privacy Policy on your part. Your continued use of the Wikimedia Sites after any subsequent version of this Privacy Policy becomes effective, following notice as outlined above, constitutes acceptance of that version of the Privacy Policy on your part.

Contact Us

If you have questions or suggestions about this Privacy Policy, or the information collected under this Privacy Policy, please email us at privacy@wikimedia.org (<mailto:privacy@wikimedia.org>) or [contact us](#) directly.

Thank You!


Thank you for reading our Privacy Policy. We hope you enjoy using the Wikimedia Sites and appreciate your participation in creating, maintaining, and constantly working to improve the largest repository of free knowledge in the world.

This privacy policy was approved by the board on April 25th 2014 and went into effect on June 6, 2014. Previous versions can be found below:

- **[Privacy policy \(November 2008 - June 2014\): effective from November 25, 2008 until June 6, 2014](#)**

- **Privacy policy (August 2008 - November 2008)**: effective from August 19, 2008 until November 25, 2008.
- **Privacy policy (June 2006 - August 2008)**: effective from June 21, 2006 until August 19, 2008.
- **Privacy policy (April 2005 to June 2006)**: effective from April 2005 until June 21, 2006

Please note that in the event of any differences in meaning or interpretation between the original English version of this Privacy Policy and a translation, the original English version takes precedence.

[Back to top](#) 

[± \(https://wikimediafoundation.org/w/index.php?title=Template:Privacy_policy_navigation_2&action=edit\)](https://wikimediafoundation.org/w/index.php?title=Template:Privacy_policy_navigation_2&action=edit)

Privacy-related pages

[Privacy policy](#) · [FAQ](#) · [Glossary of key terms](#) · [Wikimedia blog privacy policy](#) · [Subpoena FAQ](#) · [Access to nonpublic information](#) · [Data retention guidelines](#) · [Donor policy](#) · [Requests for user information](#)

Retrieved from "https://wikimediafoundation.org/w/index.php?title=Privacy_policy&oldid=113231"

This page was last edited on 14 February 2018, at 22:37.

Text is available under the [Creative Commons Attribution-ShareAlike License](#); additional terms may apply. See [Terms of Use](#) for details.

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 36

COMMUNITY

WIKIPEDIA

FOUNDATION

TECHNOLOGY

SHARE f g+ t

OPERATIONS, TECHNOLOGY

The future of HTTPS on Wikimedia projects

By Ryan Lane
August 1st, 2013

The Wikimedia Foundation believes strongly in protecting the privacy of its readers and editors. Recent leaks of the NSA's XKeyscore program have prompted our community members to push for the use of HTTPS by default for the Wikimedia projects. Thankfully, this is already a project that was being considered for this year's official roadmap and it has been on our unofficial roadmap since native HTTPS was enabled. Our current architecture cannot handle HTTPS by default, but we've been incrementally making changes to make it possible. Since we appear to be specifically targeted by XKeyscore, we'll be speeding up these efforts.

THIS ARTICLE IS AVAILABLE IN:
ENGLISH 中文

The Wikimedia Foundation believes strongly in protecting the privacy of its readers and editors. Recent leaks of the NSA's XKeyscore program have prompted our community members to push for the use of HTTPS by default for the Wikimedia projects. Thankfully, this is already a project that was being considered for this year's official roadmap and it has been on our unofficial roadmap since native HTTPS was enabled.

Our current architecture cannot handle HTTPS by default, but we've been incrementally making changes to make it possible. Since we appear to be specifically targeted by XKeyscore, we'll be speeding up these efforts. Here's our current internal roadmap:

1. Redirect to HTTPS for log-in, and keep logged-in users on HTTPS. ~~This change is scheduled to be deployed on August 21, at 16:00 UTC.~~ **Update as of 21 August:** we have delayed this change and will now deploy it on Wednesday, August 28 at 20:00 UTC/1pm PT.
2. Expand the HTTPS infrastructure: Move the SSL terminators directly onto the frontend varnish caches, and expand the frontend caching clusters as necessitated by increased load.
3. Put in engineering effort to more properly distribute our SSL load across the frontend caches. In our current architecture, we're using a source hashing based load balancer to allow for SSL session resumption. We'll switch to an SSL terminator that supports a distributed SSL cache, or we'll add one to our current solution. Doing so will allow us to switch to a weighted round-robin load balancer and will result in a more efficient SSL cache.
4. Starting with smaller projects, slowly soft-enable HTTPS for anonymous users by default, gradually moving toward soft-enabling it on the larger projects as well. By soft-enable we mean changing our rel=canonical links in the head section of our pages to point to the HTTPS version of pages, rather than the HTTP versions. This will cause search engines to return HTTPS results, rather than HTTP results.

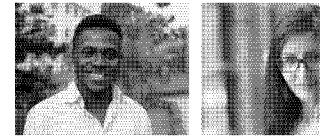
GET CONNECTED f t g+ in

GET OUR EMAIL UPDATES

Your email address

Subscribe

MEET OUR COMMUNITY



The one-man band Nigerian cinema into Wikipedia
Wikipedia is a to "plant and harvest" free knowledge: Ar Aghayan

More Community Profiles

MOST VIEWED THIS MONTH

'Monumental' winners from th world's largest photo contest showcase history and heritage

The top fifteen images from Wiki...

Türkiye'den Vikipedi'ye erişim engeli halen devam ediyor

Vikipedi'nin tüm dil sürümleri, Nisan ayını

New monthly dataset shows w people fall into Wikipedia rabl holes

The Wikimedia Foundation's Analytics tea

ARCHIVES

FEBRUARY 2018

JANUARY 2018

JA3312

- 5. Consider enabling perfect forward secrecy. Enabling perfect forward secrecy is only useful if we also eliminate the threat of traffic analysis of HTTPS, which can be used to detect a user's browsing activity, even when using HTTPS.
- 6. Consider doing a hard-enable of HTTPS. By hard-enable we mean force redirecting users from HTTP pages to the HTTPS versions of those pages. A number of countries, China being the largest example, completely block HTTPS to Wikimedia projects, so doing a hard-enable of HTTPS would probably block large numbers of users from accessing our projects at all. Because of this, we feel this action would probably do more harm than good, but we'll continue to evaluate our options here.
- 7. Consider enabling HTTP Strict Transport Security (HSTS) to protect against SSL-stripping man-in-the-middle attacks. Implementing HSTS could also lead to our projects being inaccessible for large numbers of users as it forces a browser to use HTTPS. If a country blocks HTTPS, then every user in the country that received an HSTS header would effectively be blocked from the projects.

DECEMBER 2017

NOVEMBER 2017

OCTOBER 2017

OLDER POSTS 26

WORK AT WIKIMEDIA

Work with the foundation that supports W and its sister projects around the world. A and join us

Currently we don't have time frames associated with any change other than redirecting logged-in users to HTTPS, but we will be making time frames internally and will update this post at that point.

Until HTTPS is enabled by default, we urge privacy-conscious users to use HTTPS Everywhere or Tor [1].

Ryan Lane
Operations Engineer, Wikimedia Foundation

[1]: There are restrictions with Tor; see Wikipedia's information on this.

50 Comments on The future of HTTPS on Wikimedia projects

zzo38 3 years

Can you **PLEASE** add another domain name that disables HTTPS? I want to opt-out of HTTPS and I can no longer do so.

Share

peter 3 years

Are you kidding Wikimedia?

"Consider doing a hard-enable of HTTPS. By hard-enable we mean force redirecting users from HTTP pages to the HTTPS versions of those pages. A number of countries, China being the largest example, completely block HTTPS to Wikimedia projects, so doing a hard-enable of HTTPS would probably block large numbers of users from accessing our projects at all. Because of this, we feel this action would probably do more harm than good, but we'll continue to evaluate our options here."

Because Chinese government is raping the Internet in China you do not enable HTTPS as hard-enable? Are you getting payed from Chinese government? Are you technicians that stupid? What is the reason to not hard-enable it? Because other people are doing bad things you do not the good? WTF?

Share

John Gilmore 4 years

Isn't it interesting how the Chinese government and NSA BOTH spy on users of Wikipedia?

I think Chinese users of Wikipedia should blame their government — not Wikipedia — for any problems that result from Wikipedia moving to encrypt more and more of their service. Wikipedia is solving a problem. The Chinese government is creating one.

It's too much to expect that the entire world should use Wikipedia in plaintext, letting any government or criminal spy on all the users, because a few governments infringe their citizens' right to use encryption. US citizens actively fought the US government's ban on encryption — and won, after a decade of work. Chinese citizens, it's your turn to fix your own government now. The rest of the world can't do it for you.

Share

KoshVorlon

4 years

* FOR ALL THOSE THAT WANT TO FLAME THE DEVS OVER THIS *

Yes – this change breaks Mozilla – it's already known.

I.E and Chrome still handles the change over fine.

You may need to switch over if your a firefox user (as I am).

Flaming the devs won't get this fixed faster.

Share

Ryan Lane

4 years

We have plans on testing SPDY after anonymous users are switched to HTTPS.

Share

Leirn

4 years

Will SPDY be next ?

Share

Ryan Lane

4 years

There wasn't any claim that adding HTTPS would completely alleviate our woes in this regard. This is only a first step towards the goal.

Share

Seb35

4 years

I want just to point that the History of cryptography should teach us to never over-expect the attacker don't have advanced techniques to cryptanalyse or decipher our message with some means (see the period where the cipher was the secret, or Enigma, Purple, recent attacks on TLS; even one-time pads can be broken if the key is not truly random). In this sense I find we should not claim "our infrastructure is secure and TLS is not a false sense of security" but "to the best of our knowledge, access to Wikimedia projects through TLS is secure regarding most of the currently known attacks".

Share

william gomes

5 years

éu gosto de assistir é irado

Share

Nicolas B.

5 years

Ryan,

Alas, Wikipedia blocks contributions from many proxies, and from TOR.

Ranyv,

Chinese people ≠ people in China.

Share

Int21h

5 years

Leave the Zhongwen Wikipedia behind. Let them keep their HTTP.

Advance the rest of the world into the 20th Century.

Share

300aq300aq

5 years

坚决支持!!!!!!!!!!!!!!

Share

qa003qa003

5 years

坚决反对!!!!!!!!!!!!!!

Share

Ryan Lane

5 years

So, HTTPS forces them to do traffic analysis, which makes their lives quite a bit harder. So, it's not a false sense of security, but isn't by itself a complete solution. As mentioned, newer protocols will likely help this situation, but we'll also be putting effort into making traffic analysis more difficult for our traffic. Our first priority, of course, is moving people to HTTPS.

Share

Ciara Hoyle

5 years

So much for clarity! That should read the above comment #10

Share

Ciara Hoyle

5 years

For clarity – the above comment #9, is a follow-on from my previous comment #2 on page 2

Share

Ciara Hoyle

5 years

Very interesting. Seeing as we are talking about eavesdropping by those with the resources a nation state (NSA et al.) doesn't the finger printing by traffic analysis issue also compromise the perceived privacy provided by 'vanilla' HTTPS? If so, are the measures described in the blog really just giving ourselves a false sense of privacy (regarding NSA level eavesdropping)?

Share

Walter Grassroot@zhwiki 5 years

As a 5-year Wikipedia editor, I appreciate for WMF's efforts on every promotion, including security protection. However, this attempt of moving to HTTPS on Wikimedia projects will completely destroy the Chinese community to reach all the Wikimedia programs, not only Zh-wikipedia. Since 2008, our Chinese Wikipedia has suffered governmental blocks for different reasons. Although we could access the HTTPS early 2013, the government still blocked this method to reach Wikipedia immediately, when we recommended this in public. Many Wikipedia-unfriendly governments would learn and act same as the Chinese Government on internet control – which means, if WMF act HTTPS on whole Wikimedia projects, more editors will suffered the block reflection in the world. In general, this action would setup all the Wikipedians in the opposite side of the governments. Thank you.

Share

Jsjsjs1111 5 years

Even if this "feature" is brought into practice, I would still strongly recommend you not to enable it on Chinese Wikipedia (zh), as for the reason that Quark stated. You are free to enable it elsewhere.

Share

Ryan Lane 5 years

Matt: China blocks Wikimedia projects on HTTPS currently, yes.

Share

MORE COMMENTS

Comments are closed.

WIKIMEDIA FOUNDATION

The Wikimedia Foundation, Inc is a nonprofit charitable organization dedicated to encouraging the growth, development and distribution of free, multilingual content, and to providing the full content of these wiki-based projects to the public free of charge. [Get Involved](#) | [Log In](#)

WIKIMEDIA PROJECTS

The Wikimedia Foundation operates some of the largest collaboratively edited reference projects in the world.

- WIKIPEDIA
- COMMONS
- MEDIA WIKI
- WIKIBOOKS
- WIKIDATA
- WIKINews
- WIKIQUOTE
- WIKISOURCE
- WIKISPECIES
- WIKIVERSITY
- WIKIVoyage
- WIKTIONARY

WIKIMEDIA MOVEMENT AFFILIATES

The Wikimedia projects have an international scope, and the Wikimedia movement he already made a significant impact throughout the world. To continue this success on a organizational level, Wikimedia is building an international network of associated organizations.

- WIKIMEDIA CHAPTERS
- THEMATIC ORGANIZATIONS
- WIKIMEDIA USER GROUPS

This work is licensed under a Creative Commons Attribution 3.0 unported license. Some images under CC BY-SA. [Read our Terms of Use and Privacy policy.](#) | Powered by [WordPress.com](#) VIP

5

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 37

COMMUNITY

WIKIPEDIA

FOUNDATION

TECHNOLOGY

SHARE



From by Colin, CC-BY

FOUNDATION, LEGAL, PLATFORM ENGINEERING, TECHNOLOGY, WIKIPEDIA

Securing access to Wikimedia sites with HTTPS

By Yana Welinder

Victoria Baranetsky, Wikimedia Foundation

Brandon Black, Wikimedia Foundation

June 12th, 2015

GET CONNECTED

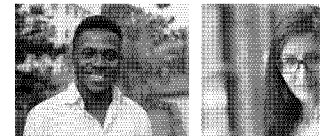


GET OUR EMAIL UPDATES

Your email address

Subscribe

MEET OUR COMMUNITY



The one-man band Nigerian cinema into Wikipedia *Wikipedia is a to "plant and harvest" free knowledge: Ar Aghayan*

More Community Profiles

MOST VIEWED THIS MONTH

'Monumental' winners from th world's largest photo contest showcase history and heritage

The top fifteen images from Wiki...

Türkiye'den Vikipedi'ye erişim engeli halen devam ediyor

Vikipedi'nin tüm dil sürümleri, Nisan ayını

New monthly dataset shows w people fall into Wikipedia rabl holes

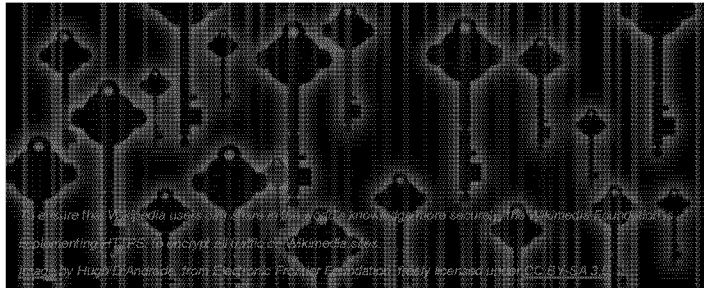
The Wikimedia Foundation's Analytics tea

ARCHIVES

FEBRUARY 2018

JANUARY 2018

The Wikimedia Foundation is happy to announce that we are implementing HTTPS to encrypt all traffic on Wikimedia sites. With this change, nearly half a billion monthly visitors on Wikipedia and its sister projects will be able to share in the world's knowledge more securely.



To be truly free, access to knowledge must be secure and uncensored. At the Wikimedia Foundation, we believe that you should be able to use Wikipedia and the Wikimedia sites without sacrificing privacy or safety.

Today, we're happy to announce that we are in the process of implementing HTTPS to encrypt all Wikimedia traffic. We will also use HTTP Strict Transport Security (HSTS) to protect against efforts to 'break' HTTPS and intercept traffic. With this change, the nearly half a billion people who rely on Wikipedia and its sister projects every month will be able to share in the world's knowledge more securely.

The HTTPS protocol creates an encrypted connection between your computer and Wikimedia sites to ensure the security and integrity of data you transmit. Encryption makes it more difficult for governments and other third parties to monitor your traffic. It also makes it harder for Internet Service Providers (ISPs) to censor access to specific Wikipedia articles and other information.

HTTPS is not new to Wikimedia sites. Since 2011, we have been working on establishing the infrastructure and technical requirements, and understanding the policy and community implications of HTTPS for all Wikimedia traffic, with the ultimate goal of making it available to all users. In fact, for the past four years, Wikimedia users could access our sites with HTTPS manually, through HTTPS Everywhere, and when directed to our sites from major search engines. Additionally, all logged in users have been accessing via HTTPS since 2013.

JA3318

Over the last few years, increasing concerns about government surveillance prompted members of the Wikimedia community to push for more broad protection through HTTPS. We agreed, and made this transition a priority for our policy and engineering teams.

DECEMBER 2017

NOVEMBER 2017

OCTOBER 2017

OLDER POSTS 26

We believe encryption makes the web stronger for everyone. In a world where mass surveillance has become a serious threat to intellectual freedom, secure connections are essential for protecting users around the world. Without encryption, governments can more easily surveil sensitive information, creating a chilling effect, and deterring participation, or in extreme cases they can isolate or discipline citizens. Accounts may also be hijacked, pages may be censored, other security flaws could expose sensitive user information and communications. Because of these circumstances, we believe that the time for HTTPS for all Wikimedia traffic is now. We encourage others to join us as we move forward with this commitment.

WORK AT WIKIMEDIA

Work with the foundation that supports W and its sister projects around the world. A and join us

The technical challenges of migrating to HTTPS

HTTPS migration for one of the world's most popular websites can be complicated. For us, this process began years ago and involved teams from across the Wikimedia Foundation. Our engineering team has been driving this transition, working hard to improve our sites' HTTPS performance, prepare our infrastructure to handle the transition, and ultimately manage the implementation.

Our first steps involved improving our infrastructure and code base so we could support HTTPS. We also significantly expanded and updated our server hardware. Since we don't employ third party content delivery systems, we had to manage this process for our entire infrastructure stack in-house.

HTTPS may also have performance implications for users, particularly our many users accessing Wikimedia sites from countries or networks with poor technical infrastructure. We've been carefully calibrating our HTTPS configuration to minimize negative impacts related to latency, page load times, and user experience. This was an iterative process that relied on industry standards, a large amount of testing, and our own experience running the Wikimedia sites.

Throughout this process, we have carefully considered how HTTPS affects all of our users. People around the world access Wikimedia sites from a diversity of devices, with varying levels of connectivity and freedom of information. Although we have optimized the experience as much as possible with this challenge in mind, this change could affect access for some Wikimedia traffic in certain parts of the world.

In the last year leading up to this roll-out, we've ramped up our testing and optimization efforts to make sure our sites and infrastructure can support this migration. Our focus is now on completing the implementation of HTTPS and HSTS for all Wikimedia sites. We look forward to sharing a more detailed account of this unique engineering accomplishment once we're through the full transition.

Today, we are happy to start the final steps of this transition, and we expect completion within a couple of weeks.

Yana Welinder, Senior Legal Counsel, Wikimedia Foundation
Victoria Baranetsky, Legal Counsel, Wikimedia Foundation
Brandon Black, Operations Engineer, Wikimedia Foundation

40 Comments on Securing access to Wikimedia sites with HTTPS

User comment box containing text: Uityyy 7 months How do I manually force unencrypted access on an old mobile browser that does not support HTTPS? I have one that 's failing to access en.m.wikipedia.org, apparently because of this, and I see no solution here. Any magic "en.insecure.wikipedia.org"? Share

Frushi 8 months

HTTPS is a 'must have' in present internet. When Google said it's gonna take a closer look for a website that don't use SSL it become clear that even websites which don't need them (because they don't have any secure infomation) will have to go to HTTPS from old http.

Share

Tom 1 year

Following the huge fail of the french ISP Orange redirecting wikipedia.fr and others, why wikipedia.fr is not protect with https/HSTS ?

http://www.theregister.co.uk/2016/10/18/orange_blow_up_french_gov_website/

Share

bart 1 year

Google usually has an alternate (cache) for each wiki link.
I just use these cache pages.

Share

Rodion 2 years

I also want there is a way to use wikipedia with plain HTTP if necessary. Currently there is a stupid debate between our government and local wiki representatives (I could not decide which of them is more stupid, I'm sorry) about restricting access to certain pages (about drugs). Providers can do this for single page if it is accessed with HTTP, but they need to deny access to whole website if it is accessed via HTTPS.

So it would be good if we have some fallback, perhaps with banner explaining "all horrible consequences" of reading wiki in plain HTTP. In my personal opinion being super-obsessed with security measures may sometimes create unwanted problems to other people :(

Share

Creg 3 years

Flo said

"Concerning privacy: when you browse Wikipedia the URLs contain the topic you are reading thus any sniffer can track what you are currently reading. Only the *contents* is encrypted, but the contents is visible by anybody anyway (in contrast to the content of my bank account)."

False. The root domain (wikipedia.org) can be inferred from the IP address of the server during the TCP/IP request but the complete URL and exact page you're reading cannot.

Read the article on https.

Share

Flo 3 years

Is there *any* way to use Wikipedia *without* https?

I have an old device which is not capable of using https. And please don't tell me to buy new hardware or software.

So please offer a possibility to read Wikipedia *without* forced https!!!!

BTW: I cannot follow the reasons to *enforce* https:

Concerning privacy: when you browse Wikipedia the URLs contain the topic you are reading (e.g.:

<https://en.wikipedia.org/wiki/CMAC>) thus any sniffer can track what you are currently reading. Only the *contents* is encrypted, but the contents is visible by anybody anyway (in contrast to the content of my bank account).

Concerning "integrity of data": nobody will guarantee that the content of Wikipedia is accurate because everybody can contribute to it. Thus I do not *fully* rely to anything I read in Wikipedia.

Share

omtim

3 years

Great step for sure, actually, in digital world https is more imperative

Share

Gary Smith

3 years

All the points are explained very clearly, Great source of information. Thanks for en-lighting us with your knowledge, it is helpful for many of us.

Share

Sports Fan Stan

3 years

All well and good to force everyone to use https. Would it be too much to ask to employ a real SSL certificate that doesn't rely on a wildcard. At present, we can't even use Wikipedia anymore because we can't trust the website. Uggghhh...

Share

astrodevamm

3 years

Very good step indeed, in fact, in cyber world https is more important because of security issues. Know a days users check website also they check that website https not. If they found https is not they click on cut button and skip from website...

Share

Pushpendra Pal

3 years

Great move team. Web is becoming a tool for governments and enforcement agencies to surveillance on citizens. SSL helps website visitors to send and receive encrypted data.

I also want to move my website <http://careervendor.com> from HTTP to HTTPS. I am fearing about loosing traffic, backlink and ranking. Can anyone please suggest a way for proper migration.

Share

astrodevamm

3 years

Very good step indeed, in fact, in cyber world https is more important because of security issues. Know a days users check website also they check that website https not. If they found https is not they click on cut button and skip from website...

Share

Ron

3 years

> There are two reasons someone might ask for any form of downgrade or opt-out to be permitted:

Make that three reasons.
 I run in DOS, and I like to keep the functionality of Arachne.

Yes, I also run Links, Elinks and Lynx in DOS, but Arachne is more versatile than all of them – except for a lack of SSL.

Share

zco38 3 years

I *really* want the ability to connect without HTTPS. I want to avoid the overhead required by HTTPS please.

Share

Mat2 3 years

“Because then a man in the middle can replace anyone’s user agent details with another user agent, and bingo, nobody any longer has any encryption at all. Invisibly and undetectably.”

Such an attack is already possible with tools such as sslstrip. Therefore user-agent sniffing doesn’t decrease security for other users out there: it will make life easier neither for criminals nor for companies that want to monitor traffic.

Wikipedia is going to use HSTS and add itself to HSTS preload lists in browsers: that will block downgrade to HTTP for new browsers.

“Upgrading from IE6 to a secure browser is entirely possible for every single user on the planet. There is no sane reason for anyone, anywhere, to use an insecure browser.”

Not every computer user can do this, unfortunately.

Google makes sure that IE6 still works:
<https://www.ssllabs.com/ssltest/analyze.html?d=google.com&s=74.125.239.96&hideResults=on>

Wikipedia is such an important site on the internet.

Share

dewimorgan 3 years

“Wouldn’t it be possible to add some user-agent sniffing” NO! No it would not. Because then a man in the middle can replace anyone’s user agent details with another user agent, and bingo, nobody any longer has any encryption at all. Invisibly and undetectably. Why would wikimedia hand attackers such a gift on a plate?

Upgrading from IE6 to a secure browser is entirely possible for every single user on the planet. There is no sane reason for anyone, anywhere, to use an insecure browser. The very worst smartphone and smartwatch in the world can browse securely. Even Lynx can handle secure browsing, and that’s been ported to just about everything.

There are two reasons someone might ask for any form of downgrade or opt-out to be permitted: 1) they are grievously uninformed; or 2) they are maliciously requesting the downgrade on behalf of some organization which wants a MitM attack to work.

One wonders how many of each group is commenting here.

Share

Mat2 3 years

Now all IE6 users will be cut off from using Wikipedia:
<https://www.ssllabs.com/ssltest/analyze.html?d=en.wikipedia.org>

Wouldn’t it be possible to add some user-agent sniffing so that these browsers could still access Wikipedia? They are usually used by poorer people.

Share

Ron Clarke 3 years

Steve,
> Why now adding a SSL/TLS support to that browser instead, is this really something very hard to do, or just not a priority?

Adding SSL to Arachne would be wonderful, and we wish we could. But.....we have a lack of suitably skilled coders with an interest in DOS browsers, and Arachne in particular.

Any volunteers ?

Share

dewimorgan 3 years

@Glenn McCorkle and Ron Clarke:

"Ron & I are active developers of DOS Arachne"

This ship has sailed.

Every single .gov domain will be HTTPS-only by next year. Many already are.

For active developers of web browsers which don't support HTTPS, implementing it should have been the number one priority for the last few years, because other browsers – even other command-line browsers that can run on legacy hardware – support it just fine. Like an FTP program without FTPS or SFTP, or an email program without STARTTLS, you'll lose market share and relevance.

Oh, and IPv6 URLs are a thing now, too.

Share

MORE COMMENTS

Comments are closed.

WIKIMEDIA FOUNDATION

The Wikimedia Foundation, Inc is a nonprofit charitable organization dedicated to encouraging the growth, development and distribution of free, multilingual content, and to providing the full content of these wiki-based projects to the public free of charge. [Get Involved](#) | [Log In](#)

WIKIMEDIA PROJECTS

The Wikimedia Foundation operates some of the largest collaboratively edited reference projects in the world.

- WIKIPEDIA
- WIKIDATA
- WIKISPECIES
- COMMONS
- WIKINEWS
- WIKIVERSITY
- MEDIAWIKI
- WIKIQUOTE
- WIKIVOYAGE
- WIKIBOOKS
- WIKISOURCE
- WIKTIONARY

WIKIMEDIA MOVEMENT AFFILIATES

The Wikimedia projects have an international scope, and the Wikimedia movement he already made a significant impact throughout the world. To continue this success on a organizational level, Wikimedia is building an international network of associated organizations.

- WIKIMEDIA CHAPTERS
- THEMATIC ORGANIZATIONS
- WIKIMEDIA USER GROUPS

This work is licensed under a Creative Commons Attribution 3.0 unported license. Some images under CC BY-SA. [Read our Terms of Use and Privacy policy.](#) | Powered by [WordPress.com](#) VIP

5

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 38

Case 1:15-cv-00662-TSE Document 168-42 Filed 12/18/18 Page 2 of 3

From: Mark Bergsma
To: Faidon Liambotis
Sent: 5/23/2014 1:16:25 PM
Subject: Fwd: Ops Goals: Questions/Expectations

Begin forwarded message:

From: Erik Moeller <erik@wikimedia.org>
Subject: Ops Goals: Questions/Expectations
Date: 23 May 2014 10:19:54 GMT+2
To: Mark Bergsma <mark@wikimedia.org>

Hi Mark,

For the goalsetting process, I'm drafting a set of questions/expectations for each team. I'll share the whole document with EMGT later, but wanted to send you the ops piece upfront just so you can take a quick spin through it. Any quick reactions welcome :)

I'd like to publish this as a subpage to the goals page once it's gone through a first pass EMGT review. The intent of this is to spur some specific thinking, but also get on the same page on the things we feel we must accomplish in the coming year. You can have conversations about this with me, with your team, or with others in the org, as you see fit.

Erik

Site Operations

Questions

- Will we be able to achieve full failover capability from EQIAD to CODFW? Should we set a goal such as quarterly failover tests? (How do we avoid a situation like with TPA where we lost failover capability?) What's the plan for CODFW utilization beyond as a secondary?
- Can we articulate goals related to use of virtualization in our infrastructure beyond Labs?
- Do we intend to plan out any additional caching location(s)? If so, can we articulate expected user benefit?
- Do we intended to implement off-site backups beyond cross-DC copies? If so, when?
- Can we establish some metrics for ongoing high-level reporting (uptime/outages/latency by service/geography etc.)?

Expectations

- 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 PFS
 - enabling IPSEC
 - investigating techniques to defeat traffic detection
 - making a definitive decision on whether to force HTTPS for all users.Let's try to attach a rough timetable to relevant objectives.

Wikimedia Labs

JA3326

Questions

- What additional data/computing resources/services should we aim to make available to the Labs community? How can we accomplish that (are there cross-functional dependencies, e.g. with analytics)?
- What infrastructure improvements are going to get us the largest bang for the buck in terms of stability/performance improvements?
- Are there needs by other teams (e.g. release engineering) that aren't currently met effectively with the Labs infrastructure? (Example: improved automatic provisioning of Labs VMs for parallelized unit test execution - multiple changesets/branches). If so, how should these needs be met? If not, how do we minimize wheel-reinvention by other teams?
- How can we more consistently showcase awesome Labs community innovations? Are there better ways to interface with the grantmaking team to ensure volunteers receive financial support as appropriate?

Expectations

- I would like us to begin articulating a more compelling vision for the lifecycle of community innovations. We've improved on the toolserver situation, but we could still do better along the following dimensions:
 - discoverability of tools
 - integration of tools into the main site experience
 - better support for Labs->Production migration where appropriateWe may not be able to resource a more comprehensive "Labs vision" yet, but we should at least begin articulating it and defining the steps we would need to take to get there (e.g. form a cross-functional team including MW core/API & UX expertise).
- Let's think about two staffing scenarios: 1) serving the core Labs purpose well, 2) raising the bar and creating a larger vision for Labs consistent with the above. What would those scenarios translate to in terms of additional FTEs and their skillsets? If the ideal Labs team is a cross-functional one, let's start having that conversation.

--

Erik Möller

VP of Engineering and Product Development, Wikimedia Foundation

—

Mark Bergsma <mark@wikimedia.org>

Lead Operations Architect

Director of Technical Operations

Wikimedia Foundation

JA3327

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 39

Enable IPsec between datacenters

Closed, Resolved
 Public

Description

Traffic between our datacenters goes across fibers that are potentially surveilled. Since we terminate HTTPS immediately at the first hop, this means that user traffic gets across to the main datacenter in cleartext.

Details

Reference rt3536

Related Objects

Task Graph	Mentions	Status	Assignee
		<input type="checkbox"/> Duplicate	None
		<input checked="" type="checkbox"/> Resolved	• Gage
		<input checked="" type="checkbox"/> Resolved	BBlack

Tags

- Interdatacenter-IPsec
- Traffic (Done)
- Operations

Subscribers

Matanya, faidon, greg and 9 others

Tokens

Assigned To

- Gage

Authored By

- rtimport, Sep 11 2012



- **rtimport** added a project: **ops-core**. Dec 18 2014, 1:23 AM
- **rtimport** raised the priority of this task from to *Normal*.
- **rtimport** set Reference to rt3536.
- **rtimport** created this task. Sep 11 2012, 5:20 PM

faidon added a comment. Sep 11 2012, 9:07 PM

On Tue, Sep 11, 2012 at 05:20:36PM +0000, Ryan Lane via RT wrote:


Traffic between esams and the US datacenters goes across the WAN. This means HTTPS isn't actually encrypted for esams users. Also, we're sending IP information across the WAN, which is privacy information.

Having IPsec tunnels between esams and the US means we're going to have a lower MTU which is going to be a constant PITA. IPsec is also hard and difficult to debug. I'd much prefer doing something like


stunnel or
pound and use plain ol' HTTPS.
Regards,
Faidon

 • **rtimport** added a comment.
Sep 11 2012, 9:07 PM

Status changed from 'new' to 'open' by RT_System

 **tstarling** added a comment.
Jul 8 2013, 11:29 PM

For users geolocated in Europe, HTTPS connections are terminated in esams and then the requests are forwarded unencrypted to eqiad. 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.

 **mark** added a comment.
Jul 9 2013, 8:46 AM


On Mon Jul 08 23:29:10 2013,
tstarling wrote:


For users geolocated in Europe, HTTPS connections are terminated in esams and then the requests are forwarded unencrypted to eqiad. 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.

Not just esams. Any link that leaves our data centers is equally suspect. So that also includes pmtpa vs eqiad, and soon ulsfo. Dedicated ipsec hardware is not very practical for this, and also pretty expensive. But I'd like to experiment with ipsec host-to-host (which is really what it was meant for) at some point...

--
Mark Bergsma <mark at wikimedia>
Lead Operations Architect
Wikimedia Foundation

 • **rtimport** added a comment.
Jul 9 2013, 8:46 AM
Status changed from 'new' to 'open' by RT_System

 **mark** added a comment.
Jul 9 2013, 8:46 AM
Queue changed from procurement to core-ops by mark

 **mark** added a comment.
Jul 9 2013, 9:06 AM
On Tue Jul 09 08:46:08 2013, mark wrote:
Dedicated ipsec hardware is not very practical for this, and also pretty expensive. But I'd like to experiment with ipsec host-to-host (which is really what it was meant for) at some point...
I'd like to (re)try IPsec in Linux with ESP in "transport mode".

The advantage here is that this doesn't need any routing changes, and avoids the significant complication of rerouting (all) traffic between these hosts with separate (policy) routing, which tends to break things for traffic that is not supposed to use the tunnel/VPN. In transport mode we can select exactly which traffic (payload only) we want to encrypt, and not the rest. We're already getting MPLS transport to esams to avoid some of this, but that doesn't (really) solve the encryption problem. If ESP in transport mode works well, that would solve it in a scaleable way. Fortunately we have sufficient configuration management in place that maintaining such a setup across many hosts is no longer a problem. With our MPLS links we'll be able to do Jumbo frames, so we will even be able to support MTU 1500 and up with IPsec. I've used IPsec with Linux about 10 years ago, and it had some problems then - especially in a mixed environment with other vendors such as Cisco routers. Rekey failures and negotiation problems. I'm hoping the

situation is better
now, especially in a uniform
Linux environment.

--

Mark Bergsma <mark at
wikimedia>
Lead Operations Architect
Wikimedia Foundation

 **faidon** added a comment. ▼

Jul 9 2013, 10:47 AM

On Tue, Jul 09, 2013 at
09:06:08AM +0000, Mark
Bergsma via RT wrote:

*We're already getting MPLS
transport to esams to avoid
some of this,
but that doesn't (really) solve
the encryption problem. If
ESP in
transport mode works well,
that would solve it in a
scaleable way.
Fortunately we have
sufficient configuration
management in place that
maintaining such a setup
across many hosts is no
longer a problem. With
our MPLS links we'll be able
to do Jumbo frames, so we
will even be
able to support MTU 1500
and up with IPsec.*

I don't have access to the
contract but I asked Leslie
yesterday and she

said that our yet-to-be-established link will have an MTU of 1514.

I've used IPsec with Linux about 10 years ago, and it had some problems then - especially in a mixed environment with other vendors such as Cisco routers. Rekey failures and negotiation problems. I'm hoping the situation is better now, especially in a uniform Linux environment.

I've tried to use it a few years back with Linux and it was incredibly messy. The software might have improved since, but I still expect a full dual-stack IPsec setup in transport mode between with two/three datacenters to be non-obvious in many ways and possibly fragile. An alternative would be to just do SSL, e.g. via stunnel. That also has a number of complexities, though. Personally, I'd much rather prefer encryption be transparent to the hosts and be handled entirely on the network equipment level.
Faidon



tstarling added a comment.

Jul 9 2013, 12:41 PM

On Tue Jul 09 08:46:08 2013, mark wrote:

Dedicated ipsec hardware is not very practical for this, and also pretty expensive. But I'd like to experiment with ipsec host-to-host (which is really what it was meant for) at some point...

This ticket came out of an IRC discussion:

<TimStarling> LeslieCarr: any guess what the cost of said equipment would be?

my googling has not yet been successful

<LeslieCarr> memory fails me : (if you open a ticket we can get some quotes

mark added a comment.



Jul 9 2013, 12:55 PM

On Jul 9, 2013, at 12:47 PM, "Faidon Liambotis via RT" <core-ops at rt> :)



--

Mark Bergsma <mark at wikimedia>



Lead Operations Architect
Wikimedia Foundation

 **mark** added a comment. 
Jul 12 2013, 12:29 PM



Merged into ticket #3536 by mark

 **mark** added a comment. 
Jul 12 2013, 12:29 PM



Merged into ticket #3536 by mark

 **jeremyb** added a comment. 
Aug 26 2013, 12:43 AM

AdminCc jeremyb added by jeremyb

 **tstarling** added a comment. 
Sep 10 2013, 1:11 AM

I don't understand why the MTU is important for IPsec feasibility. If it's only for internal traffic, then MTU discovery will be efficient and reliable, right? If we're just talking about the small performance loss due to lower TCP window size etc., then surely that is better dealt with on a separate ticket, independently of IPsec.

tstarling added a comment.

Nov 1 2013, 10:43 AM

[http://www.washingtonpost.com/world/security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html?](http://www.washingtonpost.com/world/security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html?hpid=z1)

[hpid=z1](#)

According to the a recent leak from Edward Snowden, the NSA has already been using links between Google datacentres to collect private information in plaintext, so it's not a big jump to imagine that they are doing it with us too.



coren added a comment.

Nov 1 2013, 2:00 PM

On Tue Jul 09 08:55:07 2013, mark wrote:


How about we try Linux IPsec, since it doesn't cost anything and isn't much work either. If it still sucks today, we can still buy expensive boxes or use stunnel... :)


I agree with Mark without hesitation here; the Linux ipsec


implementation is comparably robust to any hardware available, would be relatively simple to deploy thanks to configuration management and costs us little but time to deploy experimentally. Interestingly enough, I've used a simplified ipsec setup in the past where, since our endpoints were fixed, we simply used configuration management deployed keys (i.e.: no IKE) to great effect. With a bit of automation for key rotation, this meant rock-solid host to host IPsec with no dependency on networking or an externally maintained daemon to be stable -- at the cost of having to do key management ourselves (which we did through ssh). [in case you are curious, the use case included boxes deployed in networks presumed hostile and also integrated with TPM which should be unneeded in our case]


The advantage of doing it this way is that there is no capital investment required, no routing changes needed at all, and only hosts pairs we deem necessary need use IPsec at all; it's easy to deploy and


experiment on a subset of hosts.


 • **Gage** merged a task: **Restricted Task**.
Dec 18 2014, 6:51 PM

 • **Gage** claimed this task.


 • **Gage** added a subscriber:
• **rtimport**.



 **faidon** renamed this task from *Enable IPSec between esams and US datacenters* to *Enable IPSec between datacenters*.
Dec 22 2014, 9:40 AM

 **faidon** updated the task description. (**Show Details**)

 **faidon** raised the priority of this task from *Normal* to *High*.

 **faidon** set Security to None.

 **Aklapper** added a subscriber: **tstarling**. Dec 22 2014, 8:52 PM

 • **Gage** added a comment. 
Dec 24 2014, 3:45 PM

Decisions have been made to use:

- Host-to-host connections between Varnish nodes in cache sites and those in main colos
- Transport mode (ESP without AH): only the payload is encrypted;

```
IP/TCP headers are not
authenticated
• Strongswan daemon for
  ISAKMP
• IKEv2 via reuse of Puppet
  client's SSL certs + keys
• Assumption: nodes will run
  Ubuntu 14.04

Current status:

• A test setup is running
  between
  (berkelium|curium).eqiad
  and (cp3001|cp3002).esams
  in transport mode
  • Manual configuration,
    derived from
    http://www.strongswan.
    transport/
  • Hosts are sending
    syslog events to
    Logstash

• Connection resilience
  tested: 10% packet loss in
  each direction on berkelium
  • sudo iptables -A
    OUTPUT -d
    cp3001.esams.wmnet
    -m statistic --mode
    random --probability
    0.1 -j DROP
  • sudo iptables -A INPUT
    -s cp3001.esams.wmnet
    -m statistic --mode
    random --probability
    0.1 -j DROP
  • 10MB/sec throughput
    over IPsec tests
    complete successfully:
    iperf -c
```

berkelium.eqiad.wmnet
-b 10M

- Puppet module under development in 'ipsec' project in Labs
 - <https://gerrit.wikimedia.org/r/#/c/1000000/1>
 - puppetmaster: ipsec-pm.eqiad.wmflabs
 - module: ipsec-pm:/var/lib/git/operatio
 - 12.04 clients: (ipsec-c1|ipsec-c2).eqiad.wmflabs
 - 14.04 clients: (ipsec-c3|ipsec-c4).eqiad.wmflabs

Remaining tasks:

- Improve reusability of puppet module
 - Support Ubuntu 12.04 which has /etc/init.d/ipsec instead of /etc/init/strongswan.c
 - Support Debian Jessie which has /etc/init.d/ipsec
 - remove varnish node assumptions so that it can be used between any two nodes
 - remove wmf-specific dependencies so that it may be used outside of the org
 - make it work in Labs
 - achieve better code/data separation

- remove dependency on role::cache::configuration
- Specify connections by IP rather than hostname in order to support IPv4 + IPv6 (SAs must be configured for each)
- Possibly restrict encryption to Varnish traffic using configuration parameters leftsubnet/rightsubnet which allow port specification
- Consider application of IPsec to non-Varnish inter-colo traffic
- Possibly add corresponding firewall rules to enforce use of IPsec

Problem:

- Configuration requires at least one side of a connected pair of hosts to specify the remote hostname (and v4 + v6 IPs, for our purposes)
- This means that the config file template in the puppet module must enumerate remote hosts
- This information is not currently available via facter or hiera
- Therefore we need a way to query for that list of nodes and their IPs
- Inspired by modules/torrus/templates/v


from
manifests/role/cache.pp

- However that does not have clean code/data separation, and v4 + v6 IPs are not included

Solution?:

- Store data in Hiera:
hostname, IPv4 address, IPv6 address, site and cluster membership for at least Varnish nodes

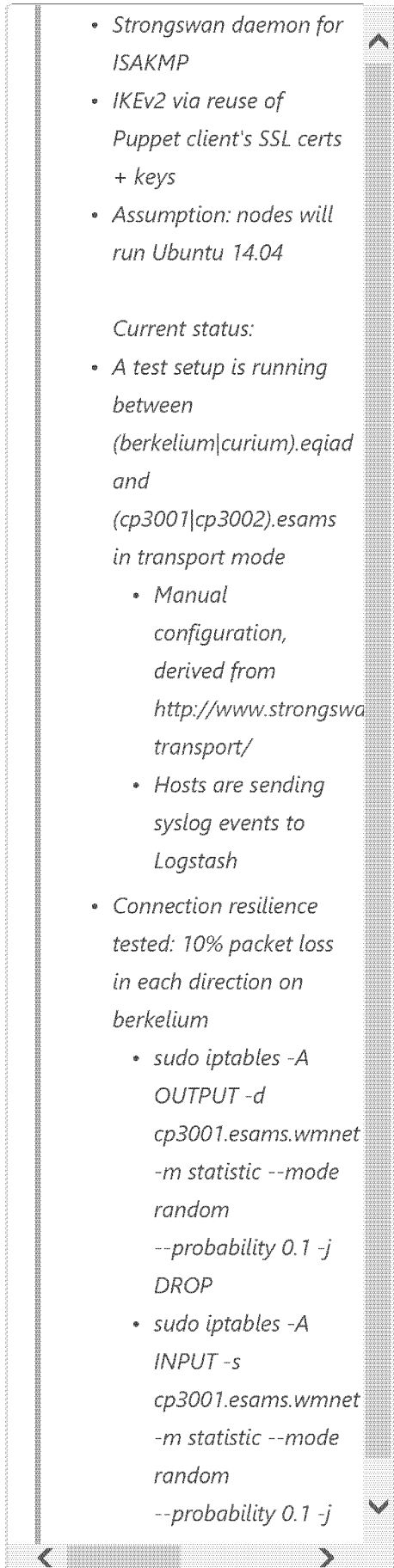
Documentation under development (to be moved to Wikitech):
[https://office.wikimedia.org/wiki/Use\(WMF\)/IPsec](https://office.wikimedia.org/wiki/Use(WMF)/IPsec)

 **mark** added subscribers:

- **Gage, mark.**
Dec 29 2014, 1:47 PM

In **T81543#943073**,
○ **@Gage** wrote:
Decisions have been made to use:

- *Host-to-host connections between Varnish nodes in cache sites and those in main colos*
- *Transport mode (ESP without AH): only the payload is encrypted; IP/TCP headers are not authenticated*



• Strongswan daemon for ISAKMP

• IKEv2 via reuse of Puppet client's SSL certs + keys

• Assumption: nodes will run Ubuntu 14.04

Current status:

• A test setup is running between (berkelium|curium).eqiad and (cp3001|cp3002).esams in transport mode

- Manual configuration, derived from [http://www.strongswan.org/wiki/index.php/Transport/](http://www.strongswan.org/wiki/index.php/Transport)
- Hosts are sending syslog events to Logstash

• Connection resilience tested: 10% packet loss in each direction on berkelium

- `sudo iptables -A OUTPUT -d cp3001.esams.wmnet -m statistic --mode random --probability 0.1 -j DROP`
- `sudo iptables -A INPUT -s cp3001.esams.wmnet -m statistic --mode random --probability 0.1 -j`

- 10MB/sec throughput over IPsec tests complete successfully: iperf -c berkelium.eqiad.wmnet -b 10M

Thanks, this is very helpful!

Remaining tasks:

- Improve reusability of puppet module
 - Support Ubuntu 12.04 which has /etc/init.d/ipsec instead of /etc/init/strongswan
 - Support Debian Jessie which has /etc/init.d/ipsec
 - remove varnish node assumptions so that it can be used between any two nodes
 - remove wmf-specific dependencies so that it may be used outside of the org
 - make it work in Labs
 - achieve better code/data separation
 - remove dependency on role::cache::configurat

- *Specify connections by IP rather than hostname in order to support IPv4 + IPv6 (SAs must be configured for each)*
- *Possibly restrict encryption to Varnish traffic using configuration parameters leftsubnet/rightsubnet which allow port specification*
- *Consider application of IPsec to non-Varnish inter-colo traffic*
- *Possibly add corresponding firewall rules to enforce use of IPsec*

Could you create separate Phabricator tasks for (most of) these?

*Documentation under development (to be moved to Wikitech):
[https://office.wikimedia.org/wiki/USCA4/USCA4\(WMF\)/IPsec](https://office.wikimedia.org/wiki/USCA4/USCA4(WMF)/IPsec)*

Wouldn't it be better to develop this on Wikitech directly? You can just slap a draft template on the page to indicate it's not final/production ready yet.

 • **Gage** added a comment. 

Jan 5 2015, 6:13 PM

I feel that we need greater clarity about exactly who are we protecting our traffic from and how much effort is appropriate to expend on this goal.

From an article in Ars Technica dated Dec 30 2014 (<http://ars.to/1B230yP>):

"... in 2010, the NSA had already developed tools to attack the most commonly used VPN encryption schemes: Secure Shell (SSH), Internet Protocol Security (IPSec), and Secure Socket Layer (SSL) encryption."

This article discusses PSK, which we do not use, but also IKE:

"...trying to capture IPSec Internet Key Exchange (IKE) and Encapsulating Security Payload (ESP) traffic during VPN handshakes to help build better attacks."

if that doesn't work, they try:

"...gathering more information on the systems of interest from other data collection sites or doing an end-run by calling on Tailored Access Operations to "create access points" through exploits of one of the endpoints of the VPN connection."

We must assume that this agency is not the only one with such capacity.

My question is: exactly who are we trying to secure our inter-colo communications from, and what is the feasibility of achieving that goal in the face of this information?

My impression is that adding IPsec can only potentially protect us from actors who can gain access to routers along our transit paths and record our traffic but do not have resources to apply the above methods.

 • Gage closed subtask 

Restricted Task as *Resolved*.

Jan 11 2015, 4:13 PM

 • Gage added a comment. 

Jan 12 2015, 4:51 AM

More on the 12/2014 leaked info, from a Libreswan developer: "If you configure your IPsec based VPN properly, you are not affected. Always use Perfect Forward Secrecy and avoid PreSharedKeys.":

<https://nohats.ca/wordpress/blog/2014/12/stop-using-ipsec-just-yet/>

In Strongswan: "IKEv2 always uses PFS for IKE_SA rekeying whereas for CHILD_SA rekeying PFS is enforced by defining a Diffie-Hellman dhgroup in the esp parameter.":


https://wiki.strongswan.org/projects/strongswan/wiki/IKEv2_rekeying


https://wiki.strongswan.org/projects/strongswan/wiki/CHILD_SA_rekeying


esp = <cipher suites>
The notation is encryption-integrity[-dhgroup][-esnmode]
Defaults to aes128-sha1,3des-sha1
As a responder both daemons accept the first supported proposal received from the peer.
In order to restrict a responder to only accept specific cipher suites, the strict flag (!, exclamation mark)


Currently configured value:
esp=aes256-sha512-modp4096!


Input on cipher suite selection is solicited.

 **faidon** mentioned this in **T86663: Expand HTTP frontend clusters with new hardware.** Jan 13 2015, 2:41 PM

 **Dzahn** added a subscriber: **Dzahn.** Jan 20 2015, 7:26 PM


 **BBlack** added a subscriber: **BBlack.** Jan 20 2015, 7:27 PM


 **chasemp** added a project: **Interdatacenter-IPsec.** Jan 20 2015, 7:42 PM



 **Gage** mentioned this in **rOPUP917a7be9e69a: Strongswan: IPsec Puppet module.** Mar 1 2015, 11:19 PM






Jdforrester-WMF added a subscriber: **Jdforrester-WMF**.
Mar 10 2015, 6:50 PM


 **greg** added a subscriber: **greg**.
Mar 11 2015, 2:49 AM



 **Dzahn** awarded a token.
Mar 11 2015, 3:07 AM

 • **Gage** closed subtask 
Restricted Task as *Resolved*.
Mar 13 2015, 5:35 AM


 • **Gage** closed subtask 
Restricted Task as *Resolved*.

 **BBlack** added a subtask:
T96854: Reboot caches for kernel 3.19.6 globally.
Apr 22 2015, 2:30 PM

 **BBlack** added a subtask:
T94417: Fix ipv6 autoconf issues. Apr 22 2015, 2:35 PM

 **BBlack** added a comment. 
Apr 27 2015, 8:05 PM

Where are we at on this, aside from my blockers for final rollout re: kernel updates + IPv6 SLAAC?

 **BBlack** added a parent task:
T86718: Upgrade eqiad misc varnish cluster from 2 to 4 systems. Apr 27 2015, 8:05 PM

BBlack added a subscriber: **faidon**.

May 3 2015, 11:19 PM

I've been going over the [Interdatacenter-IPsec](#) tasks today trying to get a picture of the overall situation and what's blocking various stages of deployment. This is a basic rundown of how I see things now:

I don't think we need or want crypto-traffic-only enforcement at this stage. Let's get this rolled out in a form where we still fall back to working, unencrypted traffic and simply have good monitoring in place that will alert us to this fallback condition. We can explore whether and how we want to force encryption at a later date. It could well be the case that ipsec with hostpair associations is not how we address our traffic crypto problems in the very long term view anyways. What we need now is just basically-reliable protection and alerting.

Tickets that can probably be ignored/dropped for now and not block deployment:

1. [T85823](#) - firewall rules - see above re: enforcement
2. T85827 - opportunistic encryption - seems dead-for-now upstream, so not really an available option

3. T85822 - restricting crypto to specific ports' traffic - does not seem necessary. The bastions won't be among the hostpairs involved, so SSH via them will always work fine. The traffic we'd want protected is the bulk of the traffic for any given hostpair, so efficiency isn't a big concern here either. If anything, not restricting by-port is a more secure-by-default solution anyways.

Nits that can probably easily be cleaned up / closed / ready:

1. **T96111** - Previous reauth failure investigation - seems ready to close, modulo ensuring we've discovered/applied sane runtime production values for various related parameters like lifetime and margin.
2. **T92604** - Rollout plan - seems sane, although the primary ticket text is a bit mixed/dated (we don't have it applied on all esams text caches, for instance, and wouldn't as a first step...). But yes, the general idea here to test on one hostpair only in production and then gradually enable the others is sane.
3. T95373 - Update Puppet CA cert - doesn't seem to be a

true blocker, more like "if we're going to fix this, let's do it now instead of later". Shouldn't be hard, right? If not, let's get it over with. If it is, then let's not block IPsec on it.

4. **T88536** - Implement a big IPsec off switch - core script seem to already be merged and presumably basically works? There's a followup commit dating back to ~2w ago with some nits/bugfix traffic, not yet merged. What's stalling on this?
<https://gerrit.wikimedia.org/>

Functional core IPsec things that definitely need to be working for deployment, and may need some serious work-time on them:



1. **T92603** - Monitoring - Seems we have some work here, but is missing (in my opinion) "ip xfrm" correlation, plus reviewing for smaller nits and such, and actual testing. Critical due to lack of real traffic enforcement, so that we're aware if things break down.
2. **T92602** - Stats traffic protection - Critical IMHO, as we're still leaking way too much information without this. Needs: identify the list of kafka brokers involved, figure out if they're already on jessie or

pre-req for our current working test configs), sort out puppet bits for including them in the configured hostpairs for tier2 DCs as well. If they're not jessie yet, this could be a pretty major holdup. We could go ahead without this initially just to get some protection in place, but we really need this ASAP regardless.

External blockers (not IPSec-specific, but block full production rollout):


1. **T94417** - Fix ipv6 autoconf issues - @faidon and I should be able to sort this out one way or another before the rest above is done.
2. **T96854** - cache reboots for kernel updates - We should be able to kick off this process later this week, and thus would expect completion by circa May 22 at the outside? We can overlap this with the first phases of rollout by ensuring we get a few key hosts rebooted early in the process that can be used for the initial production hostpairs.

Is there anything else missing that's not captured in all of the above?

 • **Gage** closed subtask 

Restricted Task as *Declined*.

May 4 2015, 5:43 PM

 • **Gage** added a comment. 

May 4 2015, 5:52 PM

Thanks, Brandon. I'll reply in order:

Proposed for ignore/drop:

1. **T85823: IPsec: add firewall r**

Agreed, we don't need this right now. However I suspect we'll want this someday. Not a blocker. Propose: keep open with lowest priority.

2. {T85827}: Agreed, no movement upstream. It's a nice idea which could have made configuration easier, but we've already done the config work so now this would represent a config change rather than a savings in effort. I've closed it.

3. {T85822}: I opened this per Mark's request but personally I don't think we'll ever need this. The goal was to minimize potential impact of IPsec, but as BBlack has pointed out this is sufficiently taken care of by the hostpairs in use: DNS lookups, SSH from bastions,

etc. will never be affected
by IPsec. Propose: close.

Clean up / close / ready:

1. **T96111: Strongswan: secu**

Updated. Need to import
Strongswan 5.3.0 into WMF
apt repo. Need to
determine appropriate
values for lifetime and
margin.

2. **T92604: IPsec: roll-out pl**

Updated. It seems we're in
agreement to try a pair of
upload hosts first.

3. {T95373}: I removed
Interdatacenter-IPsec tag
from this, but now I'm
having second thoughts. It
means replacing the puppet
cert on every host, because
they're signed with the CA
cert which needs
replacement. Not hard, but
also not trivial. If we do this
after IPsec roll-out,
it /should/ be as simple as
running puppet to copy the
new keys
into /etc/ipsec.d/cacerts/
and restarting Strongswan.

4. **T88536: Implement a big**

Revised patch uploaded this
morning. Needs review but
according to me it's bug-
free & ready.

Core requirements:

1. **T92603: Monitor IPsec sta**

Revised patch uploaded this

xfrm' checking and addresses syntax issues.
Review requested.

2. **T92602: Secure inter-datanet**

I agree that this is important. Kafka brokers are still on Precise, so they will need to be reinstalled. I'll talk to Otto about this.

External blockers:

1. **T94417: Fix ipv6 autoconf is**

I've tested & given my feedback in support of the token-based approach. Seems like we're waiting on feedback from Paravoid.

2. **T96854: Reboot caches for k**

This is BBlack & Moritz's issue, I agree with the plan to overlap with first phases of rollout. We need at least 3.19.3, which works with the current plan to deploy 3.19.6.

I'm not aware of any other related issues.




• **Gage** closed subtask
Restricted Task as *Declined*.
May 6 2015, 5:53 PM


• **Gage** removed a subtask:
~~**T85823: IPsec: add firewall rules.**~~


• **BBlack** closed subtask
T96854: Reboot caches for kernel 3.19.6 globally as *Resolved*.


May 26 2015, 12:47 PM



 **BBlack** closed subtask
~~T94417: Fix ipv6 autoconf issues~~ as *Resolved*.


May 28 2015, 6:53 PM


 **BBlack** removed a parent task:
~~T86718: Upgrade eqiad-misc varnish cluster from 2 to 4 systems.~~ Jun 4 2015, 12:01 AM


 **BBlack** added a parent task:
~~T101339: Expand misc cluster into cache PoPs.~~
Jun 4 2015, 12:05 AM


 **BBlack** added a subtask:
~~T92604: IPSec roll-out plan.~~
Jul 29 2015, 1:27 AM


  Restricted Application added a subscriber: **Matanya** · View Herald Transcript
Jul 29 2015, 1:27 AM



 **BBlack** mentioned this in
rOPUP86d5d45df63: enable ipsec for all codfw caches.
Jul 30 2015, 10:16 PM

 **BBlack** mentioned this in
rOPUP651418a26dca: enable ipsec for half eqiad text caches.


 **BBlack** mentioned this in
rOPUP390b3d7b7047: enable ipsec for all eqiad text caches.

 **BBlack** closed subtask
T92604: IPSec: roll-out plan
as *Resolved*.
Aug 3 2015, 3:56 PM

 **BBlack** added a subtask:
T92602: Secure inter-
datacenter web request log
(Kafka) traffic.
Aug 3 2015, 4:06 PM


 **BBlack** added a comment. 
Aug 3 2015, 4:09 PM

So, the basic cache<->cache work for tier2 is complete and functioning in practice (modulo ongoing operational improvements). We're still missing protection of other traffic (critically, kafka data, blocker added to previously merely referenced ticket), and we still have no answer for the traffic that crosses DCs through an LVS (critically in the near future: codfw caches -> eqiad appservers. Beyond that, it is desirable to let tier2-frontend caches bypass flowing through tier2-backend+tier1-backend for fixed "pass" traffic, but we're not there yet and this basically blocks it.


 **BBlack** mentioned this in
T110065: Switch codfw
caches to tier2, begin

~~pushing some traffic through them to test.~~

Aug 24 2015, 5:02 PM


 **BBlack** removed a subtask:
~~T92602: Secure inter-datacenter web request log (Kafka) traffic.~~


Aug 27 2015, 3:01 AM


 **BBlack** added a project:
Traffic.

BBlack closed this task as **Resolved.**
Aug 27 2015, 3:29 AM

I split off the last blocker as a separate Traffic-tagged ticket. It's important, but there's no clear priority vs other projects, and we may solve it without IPSec anyways. The rest of the work here has been functional for a while and it's time for this long-standing meta-task to die.

 **BBlack** moved this task from **Triage** to **Done** on the **Traffic** board. Sep 22 2015, 1:57 PM

 **faidon** changed the visibility from "**WMF-NDA** (Project)" to "Public (No Login Required)".
Dec 13 2017, 5:09 PM

 **faidon** changed the edit policy from "**WMF-NDA** (Project)" to "All Users".

Log In to Comment

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 40

Job descriptions/Traffic Security Engineer

< [Job descriptions](#)

Summary

We are looking for an Operations Engineer to join our Technical Operations team. Would you like to join the highly dynamic team that is responsible for the reliability and performance of a global top-10 website, Wikipedia?

The Technical Operations team has a very broad range of shared responsibilities. The team is globally distributed, working remotely with each other in a highly collaborative and consensus-oriented fashion. We only write and only use Open Source code wherever possible and we do the vast majority of our work in public view.

This Traffic Security position focuses more-specifically on the Security and Privacy responsibilities of our Traffic team within Operations. The Traffic team runs a private and privacy-protecting global CDN for Wikipedia and related sister projects. One of the key responsibilities of this position will be technical stewardship of our TLS termination for users at the edges of our network. We're passionate about protecting the privacy of our users against mass surveillance and manipulation, and we expect you to share that passion. If the word "ChaCha" doesn't make you think of dancing first, you might be the person we're looking for!

We'd like you to do these things:

- Protect our users' reading and editing habits from mass surveillance
- Keep our TLS infrastructure up to date in the face of evolving threats
- Keep track of the ever-changing landscape of browsers and other UAs
- Analyze and optimize our edge software infrastructure to enhance our users' experiences
- Assess and deploy newer protocols, technologies, and software as their time becomes ripe
- Deprecate older ones in a timely manner while balancing the needs of legacy clients
- Reactively respond to, and proactively engineer against, DDoS and other attacks
- Analyze and advise on application-layer security issues exposed over HTTPS
- Other related Traffic and Security/Privacy work as required

Experience we'd like you to bring to the table:

- A deep and current understanding of TLS, HTTP[S], TCP/IP, DNS, and other related protocols
- Hands-on experience working with TLS libraries and HTTP server software configuration
- A working knowledge of modern cryptography from a systems engineering point of view
- Experience working on general infrastructure and application-layer security issues
- Experience with Open Source operations tooling for configuration management, orchestration, and monitoring.
- Experience working on Open Source operations infrastructure in general
- Bachelor's degree or the equivalent in related work experience

And it would be even more awesome if you have any of these:

- Experience operating TLS-terminating reverse proxy servers at global scale
- Experience operating large web properties at a global scale
- Programmer experience writing and/or modifying network daemons and/or libraries in languages such as C, C++, Go, Python, and/or Rust

2/8/2018

- Some knowledge of Linux IPVS load-balancing
- Some knowledge of global IP routing
- Some knowledge of HTTP caching and related CDN technologies

Some public links on the current state of our TLS termination you might be interested in:

<https://grafana.wikimedia.org/dashboard/db/tls-ciphers>

[https://www.ssllabs.com/ssltest/analyze.html?](https://www.ssllabs.com/ssltest/analyze.html?d=en.wikipedia.org)

<https://wikitech.wikimedia.org/wiki/HTTPS>

Retrieved from "https://office.wikimedia.org/w/index.php?title=Job_descriptions/Traffic_Security_Engineer&oldid=223926"

This page was last edited on 9 January 2018, at 08:10.

The contents of this **Office Wiki** are confidential. Only users that have signed the Wikimedia Foundation's Confidentiality Agreement are authorized to have access.

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 41

COMMUNITY WIKIPEDIA FOUNDATION TECHNOLOGY

SHARE f g+

FREE CULTURE. FREE KNOWLEDGE. LEGAL. WIKIPEDIA

A Proposal for Wikimedia's New Privacy Policy and Data Retention Guidelines

By Michelle Paulson, Wikimedia Foundation
February 14th, 2014

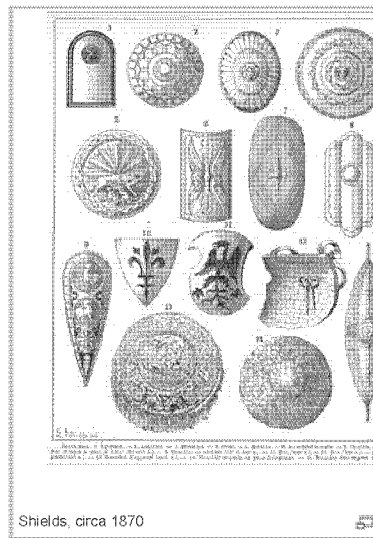
Shields, circa 1870 Privacy policies play a vital role in protecting the privacy of users. At the Wikimedia Foundation, our Privacy Policy is particularly important to us, because it is a key way we protect our users and reflect their values. It also has a broad impact, because it protects and governs the information of over twenty million registered users and 490 million monthly unique visitors. Our current Privacy Policy was approved by the Wikimedia Board of Trustees in October 2008 and has not been updated since. Given the growing concern over privacy, especially on the internet, it is important

Privacy policies play a vital role in protecting the privacy of users. At the Wikimedia Foundation, our Privacy Policy is particularly important to us, because it is a key way we protect our users and reflect their values. It also has a broad impact, because it protects and governs the information of over twenty million registered users and 490 million monthly unique visitors.

Our current Privacy Policy was approved by the Wikimedia Board of Trustees in October 2008 and has not been updated since. Given the growing concern over privacy, especially on the internet, it is important to have an updated policy which reflects both technological advances and the evolving legal issues surrounding new technology.

So, almost eight months ago, we started a conversation with the Wikimedia community about key privacy issues. Based on that conversation, we crafted a new draft Privacy Policy and introduced it to the community for feedback about five months ago. And, thanks to that feedback, we created and discussed Wikimedia's first Data Retention Guidelines. Today, we are closing the community consultations on the new draft Privacy Policy and Data Retention Guidelines. ^[1]

The new proposed Privacy Policy will now be presented to the Wikimedia Board of Trustees for review before its next meeting in April 2014. If approved, it will replace the 2008 Privacy Policy.



Shields, circa 1870

GET CONNECTED f g+ in

GET OUR EMAIL UPDATES

Your email address

Subscribe

MEET OUR COMMUNITY



The one-man band Nigerian cinema into Wikipedia *Wikipedia is a to "plant and harvest" free knowledge: Ar Aghayan*

More Community Profiles

MOST VIEWED THIS MONTH

'Monumental' winners from th world's largest photo contest showcase history and heritage

The top fifteen images from Wiki...

Türkiye'den Vikipedi'ye erişim engeli halen devam ediyor

Vikipedi'nin tüm dil sürümleri, Nisan ayını

New monthly dataset shows w people fall into Wikipedia rabl holes

The Wikimedia Foundation's Analytics tea

ARCHIVES

FEBRUARY 2018

JANUARY 2018

We would like to thank the many community members who participated in the discussions. The new proposed Privacy Policy and Data Retention Guidelines would not be what they are today without your help. (You can actually see the changes to the drafts in the Policy's and Guidelines' wiki revision histories that happened as a result of your feedback!) We received hundreds of questions, comments, and suggestions. In fact, the discussion on the Privacy Policy, along with the related Data Retention Guidelines and Access to Nonpublic Information Policy (whose consultation is also closing today) totaled approximately 195,000 words, making it longer than the Fellowship of the Ring! Together, we have created a transparent Privacy Policy draft that reflects our community's values.

DECEMBER 2017

NOVEMBER 2017

OCTOBER 2017

OLDER POSTS 26

We'd like to go over some of the ways that our new proposed Privacy Policy differs from our old Privacy Policy (the "2008 Policy"). One thing that has not changed is our goal of collecting as little information as possible, but we have made a wide variety of improvements to strengthen our commitment to users, including:

WORK AT WIKIMEDIA

Work with the foundation that supports W and its sister projects around the world. A and join us

- **More detail and transparency.** Our old Privacy Policy did not provide a great deal of specific information about what kind of data we collected or how we collected and used it. The new proposed Privacy Policy and Data Retention Guidelines explain these points in detail, so that users have a better understanding about their privacy on Wikimedia Projects.
- **The permitted use of different types of technologies.** The 2008 Policy covered IP information and cookies. The new proposed Policy, on the other hand, explains how information is collected from mobile devices, tracking pixels, JavaScript, and "locally stored data" technologies, so that we can improve the Projects.
- **Never selling user data.** The 2008 Policy doesn't mention this. While long-term editors and community members understand that selling data is against our ethos, newcomers have no way of knowing how our Projects are different from most other websites unless we tell them. The new proposed Policy spells out that we would never sell or rent their data or use it to sell them anything.
- **New glossary and FAQ.** The new proposed Policy includes a glossary that helps users familiarize themselves with wonky technical terms such as API and metadata. It also includes an FAQ to help users understand details about Wikimedia Sites, our privacy practices, and data collection technologies. For example, the FAQ provides examples of the types of technology we use to collect data, and explains to users how they can limit some of the information that is collected about them.
- **Inclusion of new activities.** We started new projects and features (like notifications, surveys, and feedback tools) after the adoption of the old Policy, so unsurprisingly the old Policy doesn't address them. The new proposed Policy explains how notifications are used and how you can opt out as well as how we may use information collected in surveys.
- **Limited data sharing.** The old Policy narrowly states that user passwords and cookies shouldn't be disclosed except as required by law, but doesn't specify how other data may be shared. The new proposed Policy expressly lists the limited ways in which all data may be shared, including with our essential volunteers. It permits providing non-personal data to researchers who can share their findings with our community so that we can understand the Projects and make them better. We have also added a Subpoena FAQ as a resource for users to learn about subpoenas generally and what they can do in the unlikely event their information is subject to a subpoena.
- **Scope of policy.** The 2008 Policy states its scope in general terms, which could be confusing or ambiguous. The new proposed Policy explains in detail when the Policy does and doesn't apply.
- **New Data Retention Guidelines.** While not formally part of the new proposed Privacy Policy, for the first time, we have a formal document, drafted in close consultation with engineering, outlining what our data retention practices are and should be. In creating these Guidelines, we tried to be as thorough as possible in specifying how long particular types of personal information will be kept.

The proposed Privacy Policy and the Data Retention Guidelines are the result of an organization-wide effort — staff from many departments helped us create these documents, and we would like to thank everyone who participated. In particular, we would like to thank Erik Möller and the entire engineering team for their continued support and participation throughout this process.

Michelle Paulson, Legal Counsel

Geoff Brigham, General Counsel

1. Although we are closing the formal community consultation on the Data Retention Guidelines, we welcome community members to continue the discussion. The Guidelines differ from policies in that they do not require approval from the Board to be implemented and can be continually updated and improved. We intend for these Guidelines to evolve and expand as time goes on.

* So many people helped us on this project. Special thanks go to Toby Negrin, Luis Villa, Dario Taraborelli, Roshni Patel, Megumi Yukie, James Alexander, and Jorge Vargas, without whom these privacy documents and consultations would not have been possible.

25 Comments on A Proposal for Wikimedia’s New Privacy Policy and Data Retention Guidelines

Sabrina Vizcaino 4 years

Valoro el hecho de querer aplicar una política de privacidad mas rígida pues muchos de los documentos de wikipedia contienen errores provocados por los mismos usuarios, aun así, creo que las opiniones de usuarios que si tengan conocimiento pleno de un tema en particular y observando su nivel de preparación académico, deberían de ser tomadas en cuenta para la perfección del documento sin que el mismo sea alterado directamente

Share

Francisco 4 years

Un saludo cordial.
Decir que no entiendo Ingles, por lo tanto no se en que términos y condiciones va a cambiar la política de privacidad de vuestra pagina WEB, a través de la encuesta realizada, es decir que querria que se tradujera tambien al Castellano o Español. At.WIKIPEDIA.....GRACIAS

Share

clarence nails 4 years

I am concerned with googles practice of listing information regarding individuals that may not be true which could damage ones reputation. Such as, information regarding disciplinary proceeding regarding an attorney that my be false without giving the affected person an opportunity to respond. Such practice should be stopped.

Share

Doctor 4 years

Some of us appreciate you all taking a clear, deliberate, and most importantly accountable policy when it comes to user security. This place in internet history is an especially murky and uncertain one, where the Utopian fools, cowboys, and salesmen have rather unflatteringly metastasised into mutually assured, multiplicitous beast. Seeded in the psychology what used to be just one of many search engines. Now obsessed with a subjective definition (and subsequent dominion) of all topology of the landscape, (to the point where many people will never understand or see beyond what has been framed for them – hypothetically: You were a Web Host or Small Business, and were refused a listing by Google at the behest of an influential agency or party. You made the robots.txt list- For a for all intents and purposes: You Do Not Exist – and you will struggle to posit a public reality the contrary) This omnivore in altruist’s clothes has created and refined both models of data aggregation, user targeted advertising and especially good at expertly deflecting any criticisms of violations of their user rights (picture of Magna Carta for internet missing : that’s a 404 jimplicit in their systems. (the same thing that seems to allow repeated gross ethical misconduct: lack of precedent or legislation makes all rights simply implied.) It is the emulation of their corporate dollar driven profiling of the ontological and semantic web, now used for and

by both the social networks (see: The flailing minutiae / cult of personality bubble) .and corporate modern web. And it is the progenitor of the worst of it. The once uninitiated NSA, now the peak of it's crypto-fascist dream. So thanks for drawing a line in the sand. It's amazing that Wikipedia still has not caved in/"Been acquired" there aren't many institutions with ethics left intact once they reach your place. Thank you. Some of us see what you are doing, and some of us are listening.

Share

Ralph Dratman 4 years

With respect to the likelihood or otherwise of a subpoena being issued against user information stored by Wikipedia, your assertion that such was "unlikely" was, I must assume, referring to the probability that any given specific user (for example, the reader of this document) would ever be subject to such. On the other hand, I'd guess the aggregate probability that some one or more users among all the wikipedia users will at some future time be subject to such subpoena is not negligible.

Share

Iola 4 years

Gracias por avisar

Share

Jonathan Pineda 4 years

Thank you.

Share

Steve 4 years

Wikipedia needs a better policy as regards transparency regarding the actions of its administrators. Some may be over zealous in some regards. It might be helpful for users to see statistics on administrative actions and be able to vote for which ones they value most and least with the objective of setting administrative limits, so many per week per administrator on the ones valued least.

Share

Sxxxx Wxxxx 4 years

I'm disappointed I didn't come across this sooner. It would have been the perfect opportunity to ONCE AGAIN voice my concern and disappointment that Wiki has gone the way of our democracy; at times to the highest bidder. Suggesting a few more fixes to cure their edit process might have helped the +90% of Wikipedia that serves its purpose...

As central a resource as Wiki is, it's not quite the incredible, compounding central database it could have been. Whether it's a policy issue or some short-coming of all wiki-s, it seems when subsequent corrections/edits don't sit well with a special interest or a corporate sponsor — even if properly annotated and referenced — changes can go missing, routinely, again and again, over months, continually, as if a well funded machine was able to maintain their talking points over the balanced and unbiased maintenance of information. All while Wikipedia sat by and did little to nothing. Public safety issues or other concerns aside, this is sides taking plain and simple, of which Wikipedia unwittingly or not has become a tool and not the right side of history we'd all expect.

It's been years since I've bothered editing, or donating (since), yet the in-depth and unbiased exposé of even the issues of plastics, Excitotoxins (MSG, Aspartame, etc), GMO, the toxic adjuvants in vaccines, and a whole host of other now common "controversies" is evidentiary and still up for grabs or a slanted treatment. Unfortunately and because of this, and completely contrary to what I'd hoped; I have to wonder

their intentions and their charitable status, while ostensibly at times a special interest driven mouthpiece for corporate sponsors...

Share

Trevor Webb

4 years

In reference to comment 13, I hope there is still some facility for correcting wicki entries. For example I am an aviation historian with 50 years experience and a masters degree and often find, usually minor, errors.

Share

levi van dijk

4 years

if you want details to be safe use pen , paper and mechanical storage. people are too lazy to "spy" or forcefully record information in books and literal files. i personally dont trust any digital information to be truly "private". im an industrialist who prefers mechanical contraptions more so than electronically functioning technology.

i guess metaphorically when referring to technology i prefer the "indomitable divide" to the "cutting edge".

Share

John Couch

4 years

Julie Krauel – the reason your school won't allow Wikipedia or any other web source to to be used is that they are not original data. The thing that is great about Wikipedia is that the reputable articles have footnotes. Go to them for your sources.

Share

Julie krauel

4 years

Why won't school allow this site for reports?

Share

Julie krauel

4 years

Mr. Crout,
What do you mean?
Jkrauel

Share

Julie krauel

4 years

Let me explain myself. I am learning more & more about the web. Especially since after being hacked of all my personal info in Oct. 13 I don't know who to hold responsible? I was simply now making a comment about Google+ note allowing you to take your name off of all "public just profile." When you have to sign up to get better apps. I would like all my info private...thank you. I will show my first name.. My kids Use your site for reports but now are banned to get any info. From you for reports. Why? I was wondering if you could tell me? Also the other apps. I. Meantioned was Google Hangouts where up to get 10 people can join in. They don't mention and listen to your calls sms as invisible??? If I wanted to spy on someone I would install that app. I was wondering not bragging on Google I was wondering if there were ways around having your info private but when it says it will be. Just as aiki said my email was kept private? WIKI not very trustworthy afterall. Great comment to make me look bad when I was wondering simply asking for help. You DEFINITELY DO NEED A NEW PRIVACY POLICY! ASAP!

Share

Julie krauel

4 years

I am not trusting of this site automatically showing my info as public just for signing in. Google makes you pretty much have too to get other apps free. Is there a way you can avoid this? I made all private but I know a lot of people that do not know about that site and handouts with invisible listeners on your calls sms beware to all these apps are spyware & sneaky!:-*

Share

James Carr

4 years

The main reason I use wikimedia is for educating myself on different subjects ! I don't use it very often, but when I do you seem to have the most useful facts on the ole inner web . Today I was searching for some army & navy info on my Uncle and Dad .I have a few unanswered questions and they're both passed on, so it being Memorial Day I thought I would try and get a little information. But with everything going on in this world of ours this day and time you can't be to careful!!!! I understand completely. Thank you, I think wikimedia is doing a great job !!!

Share

Javier ezequiel grob

4 years

Entiendo que Wikimedia sea mejor que Wikipedia, si seria mas mejor que sea privado y no en publico. Servira un mejor ejemplo que tenga mejor información en Wikimedia que en Wikipedia y que tenga los mismos idiomas o mas mejores y nuevos idiomas que los idiomas anteriores. Puede que eso sirva como un mejor ejemplo de transparencia para que todos en los paises del mundo en Sudamérica, Norteamérica, Europa, África, Asia y Oceanía (Australia). Puede que sea un mejor detalle como que este Wikimedia permita que la organización muestre el verdadero respeto hacia todos los clientes de todo el mundo y que nosotros podamos valorarlo que su privacidad pueda haber sido de una vez por todas por genuina, pero ahora es la retorica y espero que esto signifique que no esto se pueda cambiar o que esto pueda alterar toda la información proporcionada por el wikimedia.

Share

NESTOR SANTIN VELAZQUEZ

4 years

La trascendencia sin precedente de este proyecto es patente. Es como un sueño de la alfombra voladora, pero en el terreno de la ciencia y la técnica. El carácter multidisciplinario y plural, y al mismo tiempo objetivo en la construcción de contenidos no debe ser afectado, idealmente. Tampoco el carácter gratuito (No profit) aunque yo he colaborado modestamente (minúsculas cantidades de dinero) y estoy dispuesto a seguir colaborando, según mis posibilidades. Este proyecto ya es fundamental para la humanidad. Me gustaría colaborar con información de mi región y país, pero lo haría sólo en temas en los que pudiera aportar algo nuevo o desconocido. Mientras esto se materializa, gracias, gracias, gracias.

Share

Dawn Tuskey

4 years

Wow. Impressive. Wikimedia is leading by example. Never selling the little bit of info I share & you collect is a big one to me. It's gotten to the point where I'm wondering if & how I should copyright & trademark my name & other personal info.

Share

MORE COMMENTS

Comments are closed.

WIKIMEDIA FOUNDATION

The Wikimedia Foundation, Inc is a nonprofit charitable organization dedicated to encouraging the growth, development and distribution of free, multilingual content, and to providing the full content of these wiki-based projects to the public free of charge. [Get Involved](#) | [Log In](#)

WIKIMEDIA PROJECTS

The Wikimedia Foundation operates some of the largest collaboratively edited reference projects in the world.

- WIKIPEDIA COMMONS MEDIA WIKI WIKIBOOKS
- WIKIDATA WIKINEWS WIKIQUOTE WIKISOURCE
- WIKISPECIES WIKIVERSITY WIKIVOYAGE WIKTIONARY

WIKIMEDIA MOVEMENT AFFILIATES

The Wikimedia projects have an international scope, and the Wikimedia movement he already made a significant impact throughout the world. To continue this success on a organizational level, Wikimedia is building an international network of associated organizations.

- WIKIMEDIA CHAPTERS THEMATIC ORGANIZATIONS WIKIMEDIA USER GROUPS
-

This work is licensed under a Creative Commons Attribution 3.0 unported license. Some images under CC BY-SA.
Read our Terms of Use and Privacy policy. | Powered by WordPress.com VIP

⤵

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 42

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

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 43

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

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 44

wikimedia / analytics-reportcard-data

Branch: master analytics-reportcard-data / datafiles / rc_comscore_region_uv.csv Find file Copy path

milimetric Update data through December a0ee5a3 on Dec 21, 2015
4 contributors

183 lines (182 sloc) 7.57 KB

We can make this file beautiful and searchable if this error is corrected: Unquoted fields do not allow \r or \n (line 2).

```
1 date,World
  ,China,Europe,India, Latin-America,Middle-East/Africa,North-America,Asia Pacific
2 2007/12/01,226119000
  ,469000,84703000,4758000,19063000,10828000,57630000,53895000
3 2008/01/01,242554000
  ,581000,91036000,5138000,18341000,11549000,61664000,59964000
4 2008/02/01,240754000
  ,695000,87975000,5065000,20286000,11327000,61218000,59948000
5 2008/03/01,256061000
  ,669000,92283000,5200000,24542000,13337000,63518000,62380000
6 2008/04/01,261414000
  ,2288000,93642000,5079000,26347000,13634000,63827000,63963000
7 2008/05/01,263120000
  ,994000,95234000,5264000,27002000,14139000,63186000,63560000
8 2008/06/01,251502000
  ,958000,89427000,5979000,26099000,11941000,58272000,65764000
9 2008/07/01,244326000
  ,232000,86905000,5720000,23220000,11016000,57347000,65838000
10 2008/08/01,248539000
  ,1382000,83931000,6217000,26847000,11371000,59494000,66895000
11 2008/09/01,272109000
  ,2735000,98304000,6025000,28886000,12553000,64075000,68291000
12 2008/10/01,277208000
  ,2037000,102955000,5799000,27974000,13790000,66785000,65703000
13 2008/11/01,280969000
  ,2185000,106199000,6286000,27416000,13850000,65133000,68371000
14 2008/12/01,272998000
  ,2286000,105318000,6421000,22769000,15103000,63782000,66026000
15 2009/01/01,289811000
  ,1825000,112449000,6764000,22558000,15630000,67971000,71203000
16 2009/02/01,300751000
  ,2002000,117828000,6587000,27440000,18765000,65855000,70862000
17 2009/03/01,327148000
  ,2752000,126474000,7014000,34229000,21558000,66878000,78009000
18 2009/04/01,320043000
  ,3115000,119578000,6807000,33400000,20133000,70908000,76024000
19 2009/05/01,317255000
  ,2936000,118874000,7168000,33870000,19529000,69387000,75595000
20 2009/06/01,302940000
  ,4566000,112270000,7522000,33263000,16489000,64678000,76239000
21 2009/07/01,295484000
  ,3839000,108552000,7908000,29298000,16502000,66142000,74990000
22 2009/08/01,307641000
  ,3547000,111190000,8398000,33186000,17816000,68084000,77365000
23 2009/09/01,325998000
  ,2882000,123062000,8480000,35264000,18063000,71661000,77948000
24 2009/10/01,344563000
  ,3702000,128647000,9287000,36440000,22353000,73452000,83671000
25 2009/11/01,345805000
  ,3718000,129798000,9437000,36495000,22083000,75050000,82379000
26 2009/12/01,347020000
  ,3657000,129763000,9696000,31391000,24058000,77607000,84201000
```

3/14/2018

analytics-reportcard-data/rc_comscore_region_uv.csv at master · wikimedia/analytics-reportcard-data · GitHub

27 2010/01/01,364719000
,3351000,136935000,10216000,32834000,23411000,82489000,89049000

28 2010/02/01,345218000
,2935000,133807000,9865000,36414000,21680000,80940000,72378000

29 2010/03/01,370744000
,3443000,140834000,10516000,43574000,24962000,83696000,77678000

30 2010/04/01,374846000
,4081000,144087000,10923000,44286000,25146000,83792000,77535000

31 2010/05/01,388932000
,2700000,150313000,11675000,45790000,26399000,85929000,80502000

32 2010/06/01,379112000
,2613000,151013000,12373000,43826000,23611000,80393000,80269000

33 2010/07/01,360225000
,2536000,138975000,12828000,38111000,22991000,79888000,80260000

34 2010/08/01,373392000
,2829000,140560000,13187000,42303000,26220000,81295000,83015000

35 2010/09/01,398178000
,3181000,155438000,13433000,45265000,28749000,85606000,83119000

36 2010/10/01,408350000
,3156000,159384000,13674000,45152000,33049000,87359000,83406000

37 2010/11/01,410816000
,3108000,165020000,13614000,46617000,30711000,85732000,82736000

38 2010/12/01,395472000
,3372000,157837000,14004000,38738000,30852000,87087000,80958000

39 2011/01/01,413957000
,3048000,168571000,15067000,39446000,32113000,88233000,85593000

40 2011/02/01,379415000
,2664000,150775000,12960000,41411000,29722000,80038000,77468000

41 2011/03/01,400011000
,2854000,156913000,13011000,47583000,32599000,81918000,80997000

42 2011/04/01,380716000
,2866000,149211000,12801000,45108000,30272000,78234000,77891000

43 2011/05/01,411061000
,3492000,161311000,13701000,49095000,33908000,82081000,84666000

44 2011/06/01,399362000
,3960000,153883000,14163000,47203000,30985000,80753000,86539000

45 2011/07/01,393543000
,4814000,146724000,14979000,42700000,29882000,83859000,90378000

46 2011/08/01,422779000
,5163000,152109000,15944000,52983000,31749000,88277000,97661000

47 2011/09/01,454529000
,5709000,166505000,16180000,56613000,35877000,93193000,102341000

48 2011/10/01,476627000
,7386000,176918000,16019000,57210000,40119000,96252000,106128000

49 2011/11/01,474723000
,7355000,178580000,16425000,56544000,39614000,94689000,105296000

50 2011/12/01,457063000
,8803000,173496000,16425000,45235000,40068000,94413000,103851000

51 2012/01/01,482157000
,8766000,184668000,17205000,47386000,42097000,99821000,108186000

52 2012/02/01,475699000
,7886000,179385000,18771000,51425000,41056000,98049000,105783000

53 2012/03/01,489402000
,9249000,180827000,19402000,58584000,42081000,97001000,110909000

54 2012/04/01,473380000
,6666000,176376000,18688000,55227000,40589000,96664000,104524000

55 2012/05/01,492393000
,5917000,185344000,20016000,58825000,42759000,97378000,108087000

56 2012/06/01,469644000
,5890000,174151000,21031000,54654000,39560000,93676000,107603000

57 2012/07/01,451821000
,5761000,163811000,21905000,49387000,35788000,94146000,108690000

58 2012/08/01,456255000
,5602000,163167000,22027000,52510000,36327000,95824000,108428000

59 2012/09/01,474864000
,4922000,175027000,21853000,54499000,38445000,98992000,107902000

60 2012/10/01,488364000

3/14/2018

analytics-reportcard-data/rc_comscore_region_uv.csv at master · wikimedia/analytics-reportcard-data · GitHub

Case 1:15-cv-00662-TSE Document 168-48 Filed 12/18/18 Page 4 of 4

61 ,4965000,183372000,22749000,55850000,40977000,100152000,108013000
2012/11/01,484489000

62 ,4866000,184660000,22191000,54874000,41530000,97462000,105964000
2012/12/01,472552000

63 ,4457000,183718000,23339000,45777000,40802000,96966000,105288000
2013/01/01,488473000

64 ,4194000,1922293000,24140000,47216000,40429000,99277000,109258000
2013/02/01,482999000

65 ,3218000,182809000,23104000,60701000,37906000,96653000,104931000
2013/03/01,517610000

66 ,4608000,193348000,24934000,68711000,41553000,100735000,113263000
2013/04/01,516749000

67 ,7412000,190229000,24889000,69779000,41062000,100633000,115045000
2013/05/01,521767000

68 ,8173000,192353000,25892000,69932000,41620000,98666000,119197000
2013/06/01,499578000

69 ,7265000,182455000,26861000,68162000,38842000,92442000,117677000
2013/07/01,492107000

70 ,7996000,176767000,28658000,61155000,37774000,95094000,121316000
2013/08/01,496875000

71 ,7828000,176114000,28286000,67071000,38812000,94693000,120185000
2013/09/01,505904000

72 ,6147000,184950000,27181000,68179000,39522000,96520000,116734000
2013/10/01,530471000

73 ,7900000,195496000,28677000,72075000,42520000,99543000,120838000
2013/11/01,532699000

74 ,8437000,202097000,28160000,70864000,44193000,96223000,119321000
2013/12/01,490200000

75 ,8684000,190982000,27254000,54761000,41467000,89238000,113753000
2014/01/01,495362000

76 ,7188000,199883000,27132000,54583000,41828000,85809000,113260000
2014/02/01,474139000

77 ,7981000,187029000,24917000,59520000,40603000,79780000,107207000
2014/03/01,495184000

78 ,11491000,191667000,25083000,66497000,43485000,80119000,113416000
2014/04/01,465494000

79 ,10378000,180168000,23238000,63455000,40949000,73296000,107626000
2014/05/01,468740000

80 ,10617000,180746000,23524000,66801000,42151000,69452000,109591000
2014/06/01,431791000

81 ,9408000,163846000,24116000,60494000,36908000,63512000,107030000
2014/07/01,412877000

82 ,10797000,154793000,23374000,54275000,32599000,64039000,107170000
2014/08/01,418149000

83 ,8647000,151888000,22309000,57595000,33059000,69723000,105884000
2014/09/01,440710000

84 ,7864000,163573000,21728000,62749000,34151000,74056000,106181000
2014/10/01,459745000

85 ,7706000,174682000,21563000,60589000,38294000,79394000,106785000
2014/11/01,457030000

86 ,5174000,175164000,21972000,59851000,40539000,76913000,104562000
2014/12/01,446656000

87 ,6756000,173737000,22256000,48868000,41370000,79109000,103572000
2015/01/01,455678000

88 ,6981000,177476000,22850000,48760000,41089000,81799000,106554000
2015/02/01,437387000

89 ,5480000,166126000,21435000,53495000,40387000,78353000,99026000
2015/03/01,453097000

90 ,6893000,163025000,21807000,61428000,42202000,81771000,104671000
2015/04/01,439030000

91 ,6330000,153727000,21774000,62000000,43221000,78604000,101478000
2015/05/01,430536000

,4625000,152529000,21250000,61372000,41499000,77758000,97379000

Wikimedia Foundation v. NSA
No. 15-cv-0062-TSE (D. Md.)

Plaintiff's Exhibit 45

IMMEDIATE RELEASE

NSA Stops Certain Section 702 "Upstream" Activities

Press Operations

Release No: PA-014-18

April 28, 2017

Since 2008, the National Security Agency (NSA) and other members of the U.S. Intelligence Community have relied on Section 702 of the Foreign Intelligence Surveillance Act (FISA) to conduct surveillance on specific foreign targets located outside the United States to acquire critical intelligence on issues ranging from international terrorism to cybersecurity. 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.

While the Foreign Intelligence Surveillance Court (FISC) was considering the government's annual application to renew the Section 702 certifications, NSA reported several earlier, inadvertent compliance incidents related to queries involving U.S. person information in 702 "upstream" internet collection. Although the incidents were not willful, NSA was required to, and did, report them to both Congress and the FISC. The court issued two extensions of the government's renewal application in order to receive additional information from the government about this issue and the government's plan to resolve it. The previous year's certifications remained in effect during these extension periods.

During the extension period, NSA undertook a broad review of its Section 702 program. Under Section 702, NSA collects internet communications in two ways: "downstream" (previously referred to as PRISM) and "upstream." Under downstream collection, NSA acquires communications "to or from" a Section 702 selector (such as an email address). Under upstream collection, NSA acquires communications "to, from, or about" a Section 702 selector. An example of an "about" email communication is one that includes the targeted email address in the text or body of the email, even though the email is between two persons who are not themselves targets. The independent Privacy and Civil Liberties Oversight Board described these collection methods in an [exhaustive report](#) published in 2014.

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

JA3405

intelligence target. Instead, this document will now be limited to only those communications that are directly "to" or "from" a foreign intelligence target. These changes are designed to retain the upstream collection that provides the greatest value to national security while reducing the likelihood that NSA will acquire communications of U.S. persons or others who are not in direct contact with one of the Agency's foreign intelligence targets.

In addition, as part of this curtailment, NSA will delete the vast majority of previously acquired upstream internet communications as soon as practicable.

NSA previously reported that, because of the limits of its current technology, it is unable to completely eliminate "about" communications from its upstream 702 collection without also excluding some of the relevant communications directly "to or from" its foreign intelligence targets. That limitation remains even today. Nonetheless, NSA has determined that in light of the factors noted, this change is a responsible and careful approach at this time.

After reviewing amended Section 702 certifications and NSA procedures that implement these changes, the FISC recently issued an opinion and order, approving the renewal certifications and use of procedures, which authorize this narrowed form of Section 702 upstream internet collection. A declassification review of the FISC's opinion and order, and the related targeting and minimization procedures, is underway.

The National Security Agency works tirelessly around the world to help keep the nation safe. We have a solemn responsibility and commitment to do this work exactly right. When incidents occur, we immediately report them to oversight bodies and develop appropriate solutions. We never stop putting improvements in place while carrying out our critical mission.