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

REPLY BRIEF OF PLAINTIFF–APPELLANT

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

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

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

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

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

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Other Authorities

INTRODUCTION

In FISA, Congress granted the government substantial powers to conduct foreign-intelligence surveillance of U.S. persons on U.S. soil, but it conditioned that authority on a system of judicial review and judicial remedies. Remarkably, the government now claims that the procedures Congress enacted to facilitate judicial review have no application in *any* civil lawsuit challenging FISA surveillance. Instead, it says that Congress gave effectively unilateral authority to the executive to determine who may challenge unlawful foreign-intelligence surveillance.

That was not Congress's design. Congress displaced the common-law state secrets privilege, mandating in camera review—not dismissal—when a plaintiff seeks FISA materials through discovery. It permitted plaintiffs to pursue claims for unlawful surveillance while affording the government special procedures that protect sensitive evidence. The language Congress used was broad and clear: FISA's procedures control "whenever" an aggrieved person makes "any motion or request" to "discover or obtain" FISA materials. 50 U.S.C. § 1806(f).

Despite the text, the government insists that Congress's in camera review procedures apply in one scenario only: suppression. But no court has ever adopted the government's narrow reading—not the Ninth Circuit in *Fazaga*, not the D.C. Circuit in *Barr*, not even the district court in this case. All of these courts, and

more, have recognized that plaintiffs can invoke FISA's in camera review procedures when challenging executive branch surveillance.

Congress's procedures attach here because Wikimedia is an "aggrieved person" under the statute and thus entitled to its protections. Based on the government's unprecedented disclosures about Upstream surveillance, Wikimedia has done what few plaintiffs have ever been able to do: it has plausibly alleged that it is subject to Upstream surveillance, and it has now presented extensive public evidence showing the same.

Wikimedia's evidence is plainly sufficient to overcome summary judgment. The government exaggerates Wikimedia's burden, then claims victory on the basis of an unsupported hypothetical. But Wikimedia's expert—and a score of independent technologists—have explained why some of Wikimedia's trillions of communications are copied and reviewed in the course of Upstream surveillance. Applying the correct standards to this evidence, the case should proceed.

ARGUMENT

I. Because Congress displaced the state secrets privilege in FISA cases, the district court erred in dismissing this suit on state secrets grounds.

The centerpiece of the government's argument is a strikingly narrow interpretation of Section 1806(f): it argues that this provision applies *only* in criminal cases and similar proceedings where a litigant seeks to suppress the fruits of FISA surveillance. Gov't Br. 15, 22-23. The government's argument is at odds

with the text and structure of FISA, and, if accepted, would nullify the civil remedies for unlawful surveillance that Congress established in 50 U.S.C. § 1810.

The government's arguments are also at odds with decades of civil cases endorsing or contemplating the use of Section 1806(f). *See, e.g.*, *Fazaga v. FBI*, 965 F.3d 1015, 1065 (9th Cir. 2019) (amended op.); *ACLU Found. of S. Cal. v. Barr*, 952 F.2d 457, 468 (D.C. Cir. 1991); *Mayfield v. Gonzales*, 2005 WL 1801679, at *17 (D. Or. July 28, 2005). While the government accuses Wikimedia of "discover[ing]" a novel "loophole" in the statute, Gov't Br. 1, it is the government's outlandish interpretation that has only recently been discovered. *See Al-Kidd v. Gonzales*, 2008 WL 5123009, at *5 (D. Idaho Dec. 4, 2008) (in civil suit against federal defendants, "neither party dispute[d] that section 1806(f)'s procedures are applicable" to a motion to compel).

A. Through Section 1806(f), Congress displaced the state secrets privilege in civil cases challenging FISA surveillance.

1. Section 1806(f) applies "whenever" an aggrieved person seeks to discover FISA material, not just in criminal prosecutions or suppression proceedings.

As the Ninth Circuit correctly held in *Fazaga*, 965 F.3d at 1049-52, Section 1806(f)'s in camera review procedures apply in civil challenges to FISA surveillance. The court rejected the government's radical argument that FISA's procedures govern "only when the government initiates the legal action." *Id.* at 1049. This Court should do the same. The text of the statute, the existence of

FISA's civil remedy, and the legislative history require it.

First, the text of Section 1806(f) flatly contradicts the government's argument. The statute applies "whenever" an aggrieved person makes "any" motion or request "to discover or obtain applications or orders or other materials relating to electronic surveillance *or* to discover, obtain, *or suppress* evidence or information obtained or derived from electronic surveillance." 50 U.S.C. § 1806(f) (emphases added). 50 U.S.C. § 1806(f); *Fazaga*, 965 F.3d at 1050. In arguing that Section 1806(f) is limited to suppression, the government ignores the statute's repeated use of the disjunctive to encompass *any* motion or request to discover or obtain this type of evidence. Gov't Br. 15.

Lacking textual support, the government invokes the interpretative canons of ejusdem generis and noscitur a sociis. Gov't Br. 20. Neither canon applies here because the phrase "any other statute or rule" is unambiguous. *See Conn. Nat'l Bank v. Germain*, 503 U.S. 249, 253-54 (1992); Wikimedia Br. 52-54. Even by their own terms, both canons are inapposite. Courts rely on ejusdem generis only "to ensure that a general word will not render specific words meaningless," *CSX Transp., Inc. v. Ala. Dep't of Revenue*, 562 U.S. 277, 295 (2011), and on noscitur a sociis "to avoid ascribing to one word a meaning so broad that it is inconsistent with its accompanying words," *Gustafson v. Alloyd Co.*, 513 U.S. 561, 575 (1995). Nothing in the phrase "any other statute or rule" renders other parts of Section

1806(f) "meaningless" or "inconsistent."[1]

Second, FISA's structure makes plain that Section 1806(f) applies in civil suits challenging FISA surveillance. The government's interpretation of Section 1806(f) would allow it to invoke the state secrets privilege in *every* FISA suit brought by a civil plaintiff—even in the face of extensive public evidence that the plaintiff was surveilled, and even if the government admitted the surveillance (but sought to block review of the FISA materials). This would effectively nullify the civil remedy in 50 U.S.C. § 1810. Wikimedia Br. 44-45, 52, 55; *Fazaga*, 965 F.3d at 1050-52. That Wikimedia has not brought a claim under Section 1810, Gov't Br. 31, is irrelevant to whether the government's interpretation comports with Congress's carefully designed remedial scheme.

Third, FISA's legislative history confirms that Congress intended Section 1806(f) to apply in civil challenges to FISA surveillance. Wikimedia Br. 44-45. Congress made its procedures mandatory for motions brought by an aggrieved person "*whatever* the underlying rule or statute." H.R. Rep. No. 95-1283 at 91 (1978) (emphasis added). The government cherry-picks from a Senate report to argue that the statute applies only where it has initiated litigation, Gov't Br. 20, but

[1] The government asserts that Section 1806's heading—"Use of Information"—supports its narrow reading. Gov't Br. 24. But tellingly, the heading does not say "Use of Information *by the Government*."

the Senate bill also included a civil remedy, S. Rep. No. 95-701 at 79 (1978). And unsurprisingly, the Senate's precursor to Section 1806(f) was drafted broadly enough to encompass civil discovery motions. S. Rep. No. 95-701 at 88-89. Moreover, after the Senate issued its report, the House passed its own FISA bill, which specified separate in camera review procedures for criminal cases and civil challenges. H.R. Rep. No. 95-1720 at 31-32 (1978); H.R. Rep. No. 95-1283 at 93-94 (these procedures "may not always arise in the context of suppression," and may apply to "a discovery motion in a civil trial").

Most importantly, when the Senate and House bills were reconciled at conference, the conferees "agree[d] that an in camera and ex parte proceeding is appropriate for determining the lawfulness of electronic surveillance in both criminal and civil cases." H.R. Rep. No. 95-1720 at 31-32. The conferees modified the Senate's original language to make even clearer that Section 1806(f) broadly applied to civil suits, deleting a reference to 18 U.S.C. § 3504, which applies only to efforts to suppress evidence.[2] The conferees also clarified in Section 1806(g) that if a court finds surveillance unlawful under Section 1806(f), it must either

[2] Elsewhere, the government latches onto Section 3504 to argue that Congress knew how to require the government to affirm or deny surveillance. Gov't Br. 23-24. As the government acknowledges, that provision applies in suppression proceedings, not here. If it illustrates anything, it's that Congress knew how to draft a provision to refer solely to suppression, but chose not to in Section 1806(f).

suppress evidence "*or otherwise grant the motion of the aggrieved person*." This addition, drawn from the House's bill, reflected the conferees' agreement that Section 1806(f) applied where civil plaintiffs challenge FISA surveillance. *Compare* S. Rep. No. 95-701 at 88-89, *with* H.R. Rep. No. 95-1283 at 10-11, *and* 50 U.S.C. § 1806(g) (adopting the House bill's language).[3]

This legislative record confirms the clear meaning of Section 1806's text. In displacing the state secrets privilege, Congress recognized that FISA's procedures may force the executive branch to choose between disclosing evidence or conceding to plaintiffs. H.R. Rep. No. 95-1283 at 94 ("Requirements to disclose certain information . . . might force the Government to dismiss the case (or concede the case, if it were a civil suit against it) to avoid disclosure[.]").

2. Congress clearly intended to displace the state secrets privilege in FISA cases.

As a fallback, the government contends that Congress did not speak clearly enough in Section 1806(f) to displace the state secrets privilege. Gov't Br. 31-35. That argument fails. Because the state secrets privilege is a common-law privilege, the question is whether Section 1806(f) "speaks directly" to the issue addressed by the privilege. The statute does. Wikimedia Br. 46-48; *Fazaga*, 965 F.3d at

[3] Oddly, the government cites Section 1806(g) to argue that Section 1806(f) cannot be used to determine lawfulness for purposes other than suppression. Gov't Br. 21-22. But Section 1806(g) explicitly authorizes relief *other than suppression*.

1044-48; Prof. Vladeck Amicus 13-18, ECF No. 21-1.

The government advocates a "clear statement" standard instead, but both its arguments fall flat. First, contrary to the government's claim, the state secrets privilege is a common-law evidentiary rule, not a constitutional one. *See Gen. Dynamics Corp. v. United States*, 563 U.S. 478, 485, 491 (2011) (explaining that the Court's state secrets opinion was "a common-law opinion"). This Court's opinion in *El-Masri v. United States* is entirely consistent with that conclusion. 479 F.3d 296, 303-04 (4th Cir. 2007) (explaining that the privilege "was developed at common law" and has its basis "in the common law of evidence"). While the Court recognized that the privilege "performs a function of constitutional significance," *id.*, there is no question that it is a common-law rule. *Accord Fazaga*, 965 F.3d at 1041, 1044-45 ([A]t bottom, it is an evidentiary rule rooted in common law.").

Second, the government argues that a clear-statement standard would "avoid a substantial question whether Congress may displace the privilege consistent with the separation of powers." Gov't Br. 36. But there is no question about Congress's power. Because the executive branch's authority is neither exclusive nor conclusive in this arena, Congress may displace the privilege. Wikimedia Br. 48-49. The government does not dispute Congress's power to regulate foreign intelligence surveillance affecting U.S. persons. This necessarily includes the lesser power to set the evidentiary rules that apply in civil litigation challenging

that surveillance. *See also* 50 U.S.C. §§ 1804, 1881a-c (requiring disclosure of FISA information to courts in other proceedings).

But even under a clear-statement standard, the result would be the same: FISA's clear and specific procedures displace the privilege. None of the government's cases involve a "magic words" requirement. Gov't Br. 32-33. Rather, in those cases, the courts confronted legislative records that were silent. *See Franklin v. Massachusetts*, 505 U.S. 788, 800 (1992); *Armstrong v. Bush*, 924 F.2d 282, 289 (D.C. Cir. 1991). Here, the text is clear, and there is "affirmative evidence" that Congress "considered" the separation of powers in the legislative process. *Armstrong*, 924 F.2d at 289; *see* Wikimedia Br. 47-48. Congress intended to regulate discovery of FISA-related information "notwithstanding" any other rule, having carefully weighed executive branch interests. 50 U.S.C. § 1806(f); *see, e.g.*, H.R. Rep. No. 95-1720 at 32 (Section 1806(f) "ensures adequate protection of national security interests"); S. Rep. No. 95-604 at 6, 16 (1977) ("[T]he bill recognizes no inherent power of the President in this area."); H.R. Rep. No. 95-1283 at 94 (FISA disclosure requirements may, in practice, require the executive branch to concede certain litigation). Accordingly, under either standard, FISA displaces the state secrets privilege.

B. FISA's procedures control here.

As Wikimedia has explained, Section 1806(f) applies. Wikimedia Br. 49-56.

First, Wikimedia has not only plausibly alleged that it is "aggrieved," but is one of the rare plaintiffs that has adduced evidence to support that allegation. Second, Wikimedia seeks to "discover or obtain" materials related to FISA surveillance. *Id.* Accordingly, under Section 1806(f), the government cannot rely on the state secrets privilege to withhold evidence from the court or obtain dismissal.

1. The government does not dictate whether FISA displaces the state secrets privilege.

The government contends that Section 1806(f) has not formally been "triggered" because only the DNI—not the Attorney General—has filed an affidavit describing the risks of disclosure. Gov't Br. 21, 35. But that is irrelevant to whether the state secrets privilege has been *displaced*. When an aggrieved person seeks to discover FISA-related material, as here, the basic prerequisites for Section 1806(f) are satisfied. *See Fazaga*, 965 F.3d at 1040 (observing that the plaintiffs invoked the FISA procedures). At that point, the government can no longer rely on the state secrets privilege. It may choose to proceed under either Section 1806(f) (to avoid disclosure to a plaintiff) or under the ordinary rules of civil discovery (without the state secrets privilege). But it may not circumvent FISA's protections—and obtain a state secrets dismissal—simply by declining to file the requisite affidavit.

2. Wikimedia is an "aggrieved person" under Section 1806(f).

a. Wikimedia's plausible allegations are sufficient to establish that it is "aggrieved."

As Wikimedia has explained, a plaintiff's plausible, non-conclusory allegations that it is "aggrieved" under 50 U.S.C. § 1801(k) are sufficient to satisfy the "aggrieved person" element of Section 1806(f). Wikimedia Br. 49-56; *Fazaga*, 965 F.3d at 1025, 1053.[4] Section 1806(f) applies to motions to "discover" FISA materials, and the purpose of discovery is to uncover evidence. It would be nonsensical to require a plaintiff to *prove* that it is aggrieved before the court reviews the relevant discovery under Section 1806(f). Prof. Vladeck Amicus 18-27.

In response, the government asserts that the "plausible allegations" threshold would allow "any" plaintiff to proceed under Section 1806(f). Gov't Br. 15, 25. Not so. The plausibility threshold has proven to be nearly insurmountable in practice, including in this case. *See Wikimedia Found. v. NSA*, 857 F.3d 193, 217 (4th Cir. 2017) (dismissing the complaints of eight of Wikimedia's former co-plaintiffs). Because public information about FISA surveillance is typically so

[4] The government mischaracterizes *Fazaga*'s holding. Gov't Br. 27. The *Fazaga* court observed that FISA surveillance may "drop out" of the case following in camera review if the review does not substantiate the allegations. 965 F.3d at 1067. That is consistent with predicating in camera review on plausible allegations. *Id.*; *see also* Wikimedia Br. 55-56.

scarce, the government retains substantial control over a plaintiff's ability to "plausibly" allege surveillance in the first place. But in this case, the government chose to make a series of rare disclosures about Upstream surveillance.

The government also argues that because FISA's definition of "aggrieved person" does not refer to allegations, 50 U.S.C. § 1801(k), plausible allegations cannot satisfy the aggrieved person element of Section 1806(f), Gov't Br. 24. But Section 1801(k) provides no support for that argument. Unsurprisingly, the definitions section is silent as to the *showing* required to establish that a plaintiff is aggrieved under Section 1806(f). The plausible-allegation requirement flows instead from the text and purpose of Section 1806(f), which plainly governs discovery. It flows also from Congress's intent to facilitate judicial review of unlawful executive branch surveillance.[5]

b. At most, Wikimedia must put forward prima facie evidence that it is "aggrieved," and it has done so.

Even if the Court were to conclude that a plaintiff must adduce evidence that it is aggrieved, Wikimedia has done so. *See infra* Part III. Yet the government argues that a plaintiff must definitively prove it is aggrieved before Section 1806(f)

[5] The government again invokes ejusdem generis here, Gov't Br. 24-25, but again the canon does not apply. The phrase "aggrieved person" is not a catch-all term after a list of specific items. Nor is there any ambiguity about the *meaning* of "aggrieved person"—only a dispute about the required showing under Section 1806(f). Wikimedia Br. 52-55.

applies. Gov't Br. 28-29. This argument is a wolf in sheep's clothing. If plaintiffs were required to prove that they were aggrieved before Section 1806(f) applied, the government could invoke the state secrets privilege in virtually every civil challenge to FISA surveillance. It could claim that the whole object of that threshold proceeding—determining whether the plaintiff was surveilled—was to establish a "secret" fact (just as it's done here). The government asserts that civil plaintiffs might be able to establish standing using non-privileged evidence, Gov't Br. 30, but that is disingenuous at best. The Court need look no further than the government's arguments in this case to understand the breadth of its state secrets claims.[6]

In practice, if the government were correct, the only plaintiffs who could establish that they were "aggrieved" would be those who had received an official government admission of that fact. That is contrary to the text of Section 1806, which contemplates that persons will be "aggrieved" *before* the government notifies them that they have been surveilled. 50 U.S.C. § 1806(c)-(d). And it would also allow the executive branch to dictate whether individuals subject to illegal FISA surveillance could challenge that surveillance in court. That is impossible to

[6] While the government's invocation of the state secrets privilege is subject to judicial review, Gov't Br. 30, that review is far more circumscribed than in camera review under Section 1806(f).

reconcile with Congress's intent. Wikimedia Br. 42-48, 51-52.

The government further argues that plaintiffs cannot rely on Section 1806(f) to address standing because the statute instructs courts to determine the "legality" of electronic surveillance. Gov't Br. 23. But an analysis of standing is the first step in assessing lawfulness, and the standing and merits issues here are intertwined. Wikimedia Br. 54. Moreover, the statute does not mandate the bifurcation procedure the government claims, whereby plaintiffs must *prove* they are aggrieved at a bench trial before they can proceed with *discovery*. Indeed, there is no truth to the government's claim that courts have "uniform[ly]" bifurcated standing and the merits in FISA cases. *See, e.g.*, *Amnesty Int'l USA v. McConnell*, 646 F. Supp. 2d 633 (S.D.N.Y. 2009) (at summary judgment, parties addressed standing and merits); *ACLU v. NSA*, 438 F. Supp. 2d 754 (E.D. Mich. 2006).

Nor is this case anything like *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013). Gov't Br. 25. There, the Supreme Court declined the invitation to create, out of whole cloth, an in camera proceeding that would require the government to disclose whether it is intercepting a plaintiff's communications—regardless of the plausibility of the plaintiff's allegations or the existence of its evidence. 568 U.S. at 412 n.4. Because the plaintiffs in *Clapper* did not argue that Section 1806(f) applied (or even seek discovery), and because the state secrets

privilege was not at issue, *Clapper* did not address the questions presented here.[7]

Finally, the government is incorrect that even after Section 1806(f)'s procedures apply, it "retain[s] the option to seek dismissal to protect state secrets." Gov't Br. 28. The only support the government offers is one sentence from the denial of rehearing en banc in *Fazaga*, which addresses a different scenario: where a district court orders disclosure of secret evidence *directly to the plaintiff*. *Fazaga*, 965 F.3d at 1069 n.1. This dictum, correct or not, is irrelevant to this appeal, where Wikimedia seeks in camera review by the district court. What is relevant is the *Fazaga* court's holding that Section 1806(f) displaced the state secrets privilege, and that plaintiffs can establish that they are "aggrieved" through plausible allegations. 965 F.3d at 1043-53.

C. Applying FISA's in camera review procedures would not reveal any secret evidence.

Contrary to the government's argument, Gov't Br. 25, applying Section 1806(f)'s procedures here would not require public disclosure of secret evidence. Gov't Br. 25. "[T]he FISA approach does not publicly expose the state secrets." *Fazaga*, 965 F.3d at 1048. Moreover, the details of the government's

[7] Similarly, the government's reliance on *Barr*, Gov't Br. 26-27, is misplaced. There, the court simply recognized that "in view of § 1806(f)," the government would not be required to disclose surveillance materials to a *plaintiff* in discovery. 952 F.2d at 468-69. The court, in dicta, suggested a plaintiff must meet the basic summary judgment standard before obtaining in camera review, *id.*, but Wikimedia has done so.

surveillance—*e.g.*, the identities of its targets, the specific geographic locations where Upstream surveillance is conducted, or the participating companies—are irrelevant to Wikimedia's claims and would not be disclosed by a judicial ruling. The district court need not even *review* those details to rule. Instead, the court's in camera review can cut to the chase. The court will be able to directly assess whether the NSA has been avoiding all of Wikimedia's communications (notwithstanding the public evidence), alongside any other defenses proffered by the government.

The government contends that *any* judicial ruling on Wikimedia's standing would reveal secret facts. That too is wrong. The court should apply FISA's in camera review procedures to simultaneously assess *both* standing and the merits, as the statute contemplates. If the court concludes that Wikimedia has not established standing, it could issue a brief public ruling that "Wikimedia's claims are dismissed" (alongside a redacted opinion)—which would not reveal whether Wikimedia's challenge failed on standing or on the merits. Similarly, a brief public ruling granting judgment to Wikimedia (again, alongside a redacted opinion) would simply confirm what the public evidence already shows. *See infra* Part III.

Most importantly, a ruling that Wikimedia has shown it is more likely than not that some of its communications were subject to Upstream surveillance would not endanger national security. Such a ruling would acknowledge at most three

facts, none of which risks genuine harm: (1) that, as the government has already acknowledged, Upstream surveillance involves the review of Internet communications, PCLOB Report 36-41 (JA.4: 2475-2480); (2) that, as the government has already acknowledged, Upstream surveillance involves the review of the sort of Internet communications that Wikimedia engages in—namely, "web activity," Bradner Decl. ¶¶ 314-15, 344 (JA.2: 1034-35, 1045); and (3) that Wikimedia's web traffic traverses one of the Internet circuits on which the NSA conducts Upstream surveillance, *id*. ¶ 350 (JA.2: 1047). Given the ubiquity of Wikimedia's web traffic as it communicates with hundreds of millions of individuals around the world, and the unpredictable nature of Internet routing, acknowledging this last fact would reveal nothing about the identity of the NSA's many targets or the location of the NSA's surveillance devices.

The government claims that adversaries might learn some valuable "secret," but that gets it backwards. The government is trying to avoid judicial review by asking the Court to deny what the whole world has long been able to see.

II. Even if Section 1806(f) did not apply here, the state secrets privilege would not justify dismissal of the case.

Even if the state secrets privilege applied here, reversal would still be required. The district court can rule on Wikimedia's claims on the basis of the public evidence, without disclosing privileged information. *See* Wikimedia Br. 56-62. Nonetheless, the government contends that dismissal is necessary because

(1) it could not "properly defend" itself—*i.e.*, substantiate its Wikimedia-avoidance theory—without resort to privileged evidence, and (2) litigation of Wikimedia's standing presents an unacceptable risk of disclosure. Gov't Br. 59-60. The district court accepted the government's argument without further inquiry. That was error. The court should have first assessed, in camera, whether the government's purported evidence exists at all. If the evidence does not exist, the privilege cannot attach, and further litigation cannot present any risk of disclosing state secrets. Wikimedia Br. 59-61.

The government's arguments to the contrary rest on a misreading of *El-Masri*. Gov't Br. 62. There, the Court explained that when the government invokes the state secrets privilege, "a court may conduct an in camera examination of the actual information sought to be protected." *El-Masri*, 479 F.3d at 305. Here, that in camera review was required—especially because the government sought the "drastic remedy" of dismissal, *Fitzgerald v. Penthouse Int'l, Ltd.*, 776 F.2d 1236, 1242 (4th Cir. 1985), based solely on a convoluted hypothetical at odds with its own disclosures.

The government also relies on *El-Masri* for the proposition that "hypothetical defenses," 479 F.3d at 310, can justify state-secrets dismissal, Gov't Br. 61. But this was pure dicta: the Court had already held that the plaintiff could not affirmatively establish his prima facie case. 479 F.3d at 309. And given this

Court's precedents, Wikimedia Br. 60, it is clear that *El-Masri*'s dicta does not represent a blanket endorsement of dismissal based on hypothetical claims.

The government also errs in arguing that further litigation would disclose state secrets because it would require a trial on "(i) whether NSA conducts Upstream surveillance at one or more international internet links, and (ii) whether NSA uses a 'copy-all-then-scan' approach." Gov't Br. 60. First, the government's own disclosures already answer both these questions. *See infra* Part III.

Second, resolving the question of Wikimedia's standing will not require a trial on filtering or the specifics of Upstream surveillance. If the government has no evidence to support its Wikimedia-avoidance theory, the case should simply proceed to the merits. If the government has such proof, it should submit it in camera (as *El-Masri* contemplates), so that the court can assess whether the privilege attaches. To avoid any risk that a state secrets dismissal would indirectly reveal privileged material, this Court could require the district court to evaluate standing and the merits together. *See supra* Part I.C; *Fitzgerald*, 776 F.2d at 1238 n.3 ("Often, through creativity and care," courts can "allow the merits of the controversy to be decided in some form.").

Finally, the government argues that Wikimedia has "forfeited" any challenge to the government's state secrets assertion. Gov't Br. 14 n.1. Far from it. As Wikimedia explained, when the government argues that the privilege bars the

Court from considering the public evidence—including the government's many disclosures—or from issuing a judicial ruling based on those facts, the government is wrong. Wikimedia Br. 56, 61-62 & n.20; *id.* at 35, 40 ("web activity"); *see Husayn v. Mitchell*, 938 F.3d 1123, 1132-34 & n.14 (9th Cir. 2019) (judicial finding is not equivalent to executive-branch disclosure).

III. Wikimedia's evidence that its communications are subject to Upstream surveillance is more than sufficient to defeat summary judgment.

Even if plaintiffs must present evidence of surveillance before Section 1806(f) applies, Wikimedia has done so. Wikimedia's evidence is rooted in the government's public disclosures, which show that the NSA is systematically copying and reviewing communications as they cross "international internet link[s]." Wikimedia Br. 8-12, 18-33. The government does its best to drain these disclosures of all evidentiary value, casting every single one as hopelessly ambiguous, "inchoate," or full of unknowable, secret meaning. Gov't Br. 41, 48, 51. But these public facts are not the government's alone to interpret, impervious to outside expertise or reasoned inference. *See* Evidence Professors' Amicus 19-23, ECF No. 20-1.

The summary judgment standards in this case are no different from any other. The district court was required to draw all reasonable inferences in Wikimedia's favor; credit Wikimedia's evidence as true; and assess whether Wikimedia's evidence, taken as a whole, could allow a factfinder to conclude it is

more likely than not that some of Wikimedia's communications were being copied and reviewed in 2015. Applying these standards, it is plain that Wikimedia has provided sufficient evidence to defeat summary judgment.

A. The summary judgment standard does not require Wikimedia to disprove the government's hypothetical.

The linchpin of the government's argument is its claim that the NSA could, in theory, be filtering out every one of Wikimedia's communications. The government admits that it declined to put forward *any* evidence to support this theory. Gov't Br 56. Instead, it enlisted an outside expert with "no knowledge" of the NSA's practices to dispute Scott Bradner's expert analysis. Schulzrinne Decl. ¶ 53 (JA.2: 743). Schulzrinne's declarations resemble a wild-goose chase: they describe an ever-more complex set of steps the NSA could hypothetically take to avoid all of Wikimedia's communications. *See* 2d Bradner Decl. ¶¶ 154-55 (JA.7: 3935-38) (listing the many conditions required for Schulzrinne's thought-experiment to approach reality). Meanwhile, Bradner—as well as nearly two dozen networking engineers and technologists—have explained why that hypothetical "lacks a basis in both Internet technology and engineering." Technologists' Amicus 3, ECF No. 23.

Many of the disputes between the experts are technically complex, but the Court need not resolve them here. The government's hypothetical is inadequate to support summary judgment for two overriding reasons.

First, a hypothetical possibility, no matter how elaborate, cannot overcome Wikimedia's evidence that its communications are subject to Upstream surveillance. This is black-letter law. Because a plaintiff need only establish a genuine dispute of material fact, the existence of alternate possibilities is not a valid basis for summary judgment. Fed. R. Civ. P. 56(a). Consider a case where two parties dispute whether A caused X. The plaintiff compiles an extensive record, based on public information and expert opinion, that A caused X. The defense responds solely by offering an opinion that, in theory, B *could have* caused X. That possibility would not support summary judgment. Indeed, if the government here had put forward actual evidence, at most there would be a dispute of material fact.

Second, the government badly distorts Wikimedia's burden at summary judgment. It insists that Wikimedia must demonstrate its standing either by proving absolute technological necessity, Gov't Br. 46, or by conclusively disproving each of the government's filtering scenarios (a clever way of saying the same thing). Gov't Br. 52. Both arguments are wrong. Wikimedia need not establish its standing to a certainty at summary judgment, or even at trial. Wikimedia Br. 21-22. At this stage, Wikimedia has to provide admissible evidence of its injury: the NSA's copying and review of Wikimedia's communications. That is the relevant "fact" at issue—not a particular kind of proof, technical necessity or otherwise. The

question is whether Wikimedia's evidence establishes a genuine dispute as to this injury. It does.

Nonetheless, the government suggests that Wikimedia somehow pleaded itself into a higher burden at summary judgment, and then accuses Wikimedia of "abandon[ing]" its technical allegations. Gov't Br. 47. This, too, is false. Tracking the "Wikimedia Allegation" in the Amended Complaint, Wikimedia has presented extensive evidence that, for "technical reasons," the NSA could not conduct Upstream surveillance *consistent with its public disclosures* without intercepting Wikimedia's communications. Am. Compl. ¶¶ 61-64 (JA.1: 57-58); Wikimedia Br. 22-36.

In the end, the government misdescribes the record: it claims Wikimedia conceded that a filter-first version of Upstream is technologically possible, and then presents this manufactured concession as if it were fatal.[8] *Compare* Gov't Br. 46, *with* 2d Bradner Decl. ¶¶ 114-15 (JA.7: 3919-20) ("The government treats this as a significant concession, but the government completely misrepresents how this point relates to my ultimate conclusion."). As Bradner explains, the NSA cannot be

[8] The government misleadingly quotes the district court, not Scott Bradner, as to this point. Gov't Br. 46. But the district court ignored the entire Second Bradner Declaration and improperly resolved disputes between the experts, including in this instance. Wikimedia Br. 36-40.

"filtering first" and still conducting Upstream surveillance as the government has described it. *See* 2d Bradner Decl. ¶¶ 6-58 (JA.7: 3884-3900). But *even if* one put aside the government's various disclosures, and *even if* the NSA could in theory filter-then-copy communications, Bradner explains that the NSA has overriding technical and practical reasons not to. 2d Bradner Decl. ¶¶ 115-16 (JA.7: 3919-20); Wikimedia Br. 41. This is not a concession—it is further support for Wikimedia's standing. Bradner's conclusion has since been endorsed by other network engineers and technologists. *See* Technologists' Amicus 2-4, 7-11, ECF No. 23.

B. Wikimedia has presented more than enough evidence of its standing.

1. Wikimedia has presented evidence that the NSA conducts Upstream surveillance on at least one "international Internet link" carrying Wikimedia's communications.

The government does not dispute the first prong of Wikimedia's showing: Wikimedia's trillions of communications travel every circuit carrying public Internet traffic between the U.S. and other countries. Gov't Br. 39. But on the second prong, it argues that the FISC opinion—which describes Upstream surveillance at international Internet *links*—provides no evidence that Upstream surveillance is conducted on the international Internet *circuits* that Bradner describes. For several reasons, the government is mistaken.

First, the government asserts that Wikimedia presented no evidence that an "international internet link" is a "circuit" carrying Internet traffic between the U.S.

and other countries. Gov't Br. 40-41. That is easily rejected. As Bradner explains, "international Internet link[s]" are "circuits connecting a network node in the U.S. to a network node in a foreign country." Bradner Decl. ¶¶ 225, 350 (JA.2: 1003, 1047); *see* PCLOB Report 36-37 (JA.4: 2475-76) (discussing surveillance on "circuits"). As an expert on Internet networking, Bradner is plainly qualified to opine on the technical meaning of the term "international Internet link," and the government does not dispute the well-known features of the Internet backbone. *See* Bradner Decl. ¶¶ 200-28 (JA.2: 991-1005).

Second, the government's textual argument about the meaning of the FISC opinion, Gov't Br. 40, is transparently wrong. The government says that the FISC's description of surveillance at international Internet links was "conditional" because the sentence contains the word "if"—as though the FISC were simply speculating about a theoretical possibility. But the surrounding text and context belie this reading. The FISC was describing a key feature of Upstream surveillance: its acquisition of Americans' wholly domestic communications. As the NSA "concede[d]," it will acquire Americans' communications "if the transaction containing the communication is routed through an international Internet link *being monitored* by NSA." [*Redacted*], 2011 WL 10945618, at *15 (FISC Oct. 3, 2011) (emphasis added). The routing of any individual communication is unpredictable—that's the "if." But when the FISC describes

what happens at "an international Internet link being monitored by the NSA," that is a statement of fact.

Finally, the government claims that its understanding of "international Internet link" is a state secret, Gov't Br. 41, and says that effectively bars Wikimedia's expert from relying on the FISC's opinion. But that is not how the state secrets privilege operates. While the privilege may preclude the use of *secret* evidence, *United States v. Reynolds*, 345 U.S. 1 (1953), Wikimedia is relying on *public* evidence. The district court did not rule to the contrary; rather, it held that the government could not be compelled to disclose more than was already public. JA.7: 4093-94. And ultimately, the court correctly observed that the government's other disclosures confirm that Upstream surveillance is conducted on Internet "circuits" carrying international communications. *Id.*[9]

There is no great mystery here: as Bradner explains, a "link" is a "circuit."

2. Wikimedia has presented evidence that the NSA is copying and reviewing some of its communications.

The government disputes the evidence supporting the third prong of Wikimedia's showing, but at most, the government's arguments show a material

[9] The government argues, perplexingly, that Wikimedia "forfeited" any objection to the district court's state secrets "ruling." But Wikimedia prevailed on the second prong of its showing and, in any event, the court did not "rule" that Wikimedia's public evidence was unavailable. Moreover, Wikimedia's opening brief repeatedly—and broadly—challenges the district court's state secrets rulings. Wikimedia Br. 4, 17, 56-62.

dispute of fact.

First, the government disputes Bradner's conclusion, based on the FISC opinion, that the NSA is copying and reviewing *all* communications on the international circuits it monitors. As Bradner explains, the FISC's statement that the NSA "*will acquire* a wholly domestic 'about' communication" at an international Internet link monitored by NSA is "definitive"—it "does not provide any room for any filters." 2d Bradner Decl. ¶¶ 35-36, 44 (JA.7: 3893, 3895). Yet the government maintains that the FISC's statement is consistent with its filtering hypothetical. Gov't Br. 47. But if the NSA were filtering out large categories of communications, it would have been inaccurate for the FISC to say that the NSA "*will* acquire a wholly domestic 'about' communication"—because many such communications would be filtered out and *not* acquired. 2d Bradner Decl. ¶ 42 (JA.7: 3894).

The government characterizes this as a mere semantic dispute, but it is a dispute over technical meaning and Bradner relies on his technical expertise to answer it. 2d Bradner Decl. ¶¶ 42-43 (JA.7: 3894-95). The government's reading is belied by the FISC opinion's technical precision, its careful use of different phrasing a few paragraphs away, and "other government disclosures that IP filters

are not always used." *Id.*[10]

Second, the government does not seriously dispute that it is impossible to know in advance whether any given Internet "packet" contains a selector associated with one of many moving targets. Wikimedia Br. 29-30. Yet it claims that Bradner merely speculates that the NSA is pursuing many moving targets. Gov't Br. 49. But Bradner's opinion is based on the government's disclosures, which show that the NSA had more than 120,000 Section 702 targets in 2017, and that it collected 26 *million* communications using Upstream surveillance in 2011 alone. 2d Bradner Decl. ¶¶ 75-76 (JA.7: 3906) (concluding that there are almost certainly "tens of thousands" of Upstream targets).[11] Moreover, the government's "targets" include "groups, entities, associations, corporations, or foreign powers," PCLOB Report 21 (JA.4: 2460)—reinforcing the conclusion that each target will

[10] The government asserts that the FISC's use of "may acquire" in footnote 34 refers to the "same phenomenon." Gov't Br. 48. Not so. The footnote discusses the collection of "MCTs" (multi-communication transactions), which posed one set of technical problems for the NSA; the body addresses the collection of wholly domestic "about" communications, which posed another. *See* [*Redacted*], 2011 WL 10945618, at *11 n.34, *15.

[11] Other public evidence supports Bradner's conclusion. While Section 702 involves two forms of surveillance—Upstream and PRISM—nothing prevents the NSA from pursuing the same targets using both. Indeed, the NSA almost certainly has *more* Upstream than PRISM targets because Upstream allows the NSA to acquire a far broader range of target communications by scanning Internet traffic. *See* PCLOB Report 36-41 (JA.4: 2475-80). The notion that Upstream could be limited to a tiny handful of the NSA's 100,000 targets is belied by the facts.

not be tied to a single, static address. 2d Bradner Decl. ¶ 77 (JA.7: 3907).

The experts also disagree about whether whitelisting by IP address is remotely possible. It is not. *See infra* Part III.B.3.

Third, the NSA's stated goal of acquiring its targets' communications "comprehensively" supports Bradner's conclusion that the NSA is copying all communications transiting the international internet links it monitors. Wikimedia Br. 30-36. The government's responses are without merit.

The PCLOB's observation was not a casual aside. Gov't Br. 50. As the surrounding text makes clear, the PCLOB was describing the NSA's choice of a specific *technical* implementation for Upstream surveillance, because the NSA prioritized comprehensiveness over other technical approaches that would have missed some of its targets' communications. Any other approach, the PCLOB explained, would have represented an "incomplete solution," and would have "undermine[d] confidence that communications to and from [the NSA's] targets are being reliably acquired." PCLOB Report 123 (JA.4: 2562).

The government claims that the goal of comprehensiveness might conflict with unknowable NSA priorities. But the NSA's relevant priorities are public knowledge: the NSA has made technical design choices to ensure that its targets' communications "are being reliably acquired." *Id.*; *see also* 2d Bradner Decl. ¶¶ 55-153 (JA.7: 3899-3935); Technologists' Amicus 7-19 (technical and practical

constraints overwhelmingly favor copying the entire stream of traffic on a circuit).

The government mistakenly suggests that this Court rejected any reliance on "comprehensiveness" when it rejected the Dragnet Allegation. Gov't Br. 50-51. But the Dragnet Allegation involved a very different contention: that the NSA monitored *every* international circuit. That contention is not remotely at issue now.

Finally, the government wrongly dismisses Plaintiff's corroborating evidence. Gov't Br. 51-52; Wikimedia Br. 31-32. It baldly asserts that the UK's analogue to Upstream surveillance "has no bearing on what NSA does," but the UK's disclosures corroborate Bradner's conclusion that, "[f]or technical reasons, it is necessary to intercept the entire contents of a [circuit], in order to extract even a single specific communication for examination." Bradner Decl. ¶ 368 (JA.2: 1058-59).

3. The government's Wikimedia-avoidance theory is baseless and at most presents a dispute of material fact.

The government argues that *if* the NSA were to filter communications before copying them, some contrived collection of filters might successfully screen out all of Wikimedia's communications while still capturing targets' traffic. Wikimedia's evidence shows that the government's hypothetical has no basis in reality—and, at most, creates a dispute of material fact.

Schulzrinne assumes without evidence that Wikimedia's communications are high bandwidth, *see* Bradner Decl. ¶¶ 95-96 (JA.7: 3912-13), and then

speculates that blacklisting "high-volume" websites might reduce the load on the NSA's surveillance equipment. But Schulzrinne's concerns about load are marginal because surveillance devices can process communications at the same rate that circuits can carry them. Bradner Decl. ¶ 288 (JA.2: 1024-25). At the same time, Schulzrinne's hypothetical filters "create a risk of overloading the [ISP's] router, thereby interfering with the ISP's ability to support its customers' traffic." Bradner Decl. ¶¶ 288, 363 (JA.2: 1024-25, 1051-52); *see* 2d Bradner Decl. ¶ 96 (JA.7: 3912-13).

Schulzrinne also speculates that the NSA could whitelist IP addresses other than Wikimedia's, but this is not "remotely possible." Bradner Decl. ¶ 366(d) (JA.2: 1054). The IP addresses of devices used by thousands of moving targets cannot be known in advance, and even if they could, the IP addresses on packets often have no discernible relationship to the IP addresses of the senders of the underlying communications. Bradner Decl. ¶¶ 137, 173-74, 244-47, 334 (JA.2: 971, 983, 1010-11, 1042); 2d Bradner Decl. ¶¶ 66-89 (JA.7: 3902-11). Moreover, using whitelists would require the NSA to "purposefully ignore most of the Internet," 2d Bradner Decl. ¶ 52 (JA.7: 3898), which cannot be reconciled with the government's descriptions of Upstream.

Indeed, the Technologists' Amicus Brief explains that the filtering the government hypothesizes is technically "impossible." Technologists' Amicus 19.

First, the majority of ISPs encapsulate their traffic, rendering the underlying IP addresses invisible to filters. *Id.* at 15-16; *see also* Bradner Decl. ¶¶ 124, 244-47 (JA.2: 966, 1010-11). Second, it is not possible to filter "high-volume" traffic based on IP addresses, because most large websites use "content distribution networks," which unpredictably assign proxy IP addresses to the websites whose traffic they distribute. Technologists' Amicus 16-19; *accord* 2d Bradner Decl. ¶ 84 (JA.7: 3909).

Finally, the government argues that the NSA might filter out web activity and encrypted communications, Gov't Br. 54-55, but the NSA has conceded that it collects "web activity," Bradner Decl. ¶¶ 314-15, 366(f) (JA.2: 1034-35, 1055), and that it has an interest in collecting encrypted communications for cryptanalysis, 2d Bradner Decl. ¶¶ 137-39 (JA.7: 3928-30).

At most, the government's Wikimedia-avoidance theory raises a dispute of material fact.[12]

IV. Additional harms and third-party standing

Wikimedia has shown how Upstream surveillance caused a sustained drop in readership and has required it to take costly protective measures. *See* Wikimedia

[12] The district court erred in excluding a portion of Bradner's first declaration. Wikimedia Br. 41-42; Evidence Professors' Amicus. The government makes the same error for evidence the district court *admitted*—repeatedly arguing that Bradner's opinions should simply be disregarded as "speculation." Gov't Br. 53.

Br. 63-65. The Supreme Court has recognized that such injuries are not speculative when they rest on evidence showing a substantial risk of interception. *See Clapper*, 568 U.S. at 414 n.5.

Finally, if Wikimedia has standing, it may assert the rights of its readers and contributors—whose privacy and expressive interests are also harmed by this surveillance. This is a weighty question for online communities, but the district court addressed it as an afterthought. Here, the government misconstrues the nature of the relationship required to support third-party standing, *see* Wikimedia Br. 67, and it ignores Wikimedia's evidence that users cannot bring their own suits without obstacle, *see* Temple-Wood Decl. ¶¶ 25-28 (JA.3: 2276-77). The district court erred in not crediting that evidence.

CONCLUSION

The Court should reverse the district court's orders granting the government's motion for summary judgment and denying Wikimedia's motion to compel.

Date: September 4, 2020

Respectfully submitted,

/s/ *Patrick Toomey*

Deborah A. Jeon
David R. Rocah
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND

Patrick Toomey
Ashley Gorski
Charles Hogle
AMERICAN CIVIL LIBERTIES UNION FOUNDATION

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

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

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

Counsel for Plaintiff–Appellant

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation in the Court's August 21, 2020 Order (ECF No. 38) because it contains 7,496 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f).

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word in 14-point Times New Roman.

Date: September 4, 2020

/s/ *Patrick Toomey*
Patrick Toomey
Counsel for Plaintiff–Appellant