No. 20-1191

United States Court of Appeals for the Fourth Circuit

WIKIMEDIA FOUNDATION,

Plaintiff-Appellant,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants-Appellees,

Appeal from the United States District Court
for the District of Maryland
(Case No. 1:15-cv-00662-TSE, Hon. T.S. Ellis III)

BRIEF OF PROFESSOR STEPHEN I. VLADECK AS AMICUS CURIAE IN SUPPORT OF APPELLANT

Lauren Gallo White
Wilson Sonsini Goodrich & Rosati
Professional Corporation
One Market Plaza
Spear Tower, Suite 3300
San Francisco, CA 94105
Tel: (415) 947-2000
lwhite@wsgr.com

Brian M. Willen
Wilson Sonsini Goodrich & Rosati
Professional Corporation
1301 Avenue of the Americas
40th Floor
New York, NY 10019-6022
Tel: (212) 999-5800
bwillen@wsgr.com

Attorneys for Amicus Professor Stephen I. Vladeck

July 8, 2020

TABLE OF CONTENTS

Page

STATEMENT OF IDENTIFICATION 1

INTRODUCTION 3

SUMMARY OF ARGUMENT 3

ARGUMENT 7

I. FISA DISPLACES THE STATE SECRETS PRIVILEGE 7

A. FISA, Including Section 1806(f), Was Enacted to Facilitate Judicial Oversight of Foreign Intelligence Surveillance 7

B. As the Ninth Circuit Held in *Fazaga*, Section 1806(f) Displaces the State Secrets Privilege 13

II. A PARTY WHO HAS ADEQUATELY ALLEGED STANDING TO CHALLENGE SURVEILLANCE ACTIVITY IS AN "AGGRIEVED PERSON" AUTHORIZED TO INVOKE THE *IN CAMERA* REVIEW PROCEDURE OF SECTION 1806(f) 18

A. The District Court Misapplied FISA and Effectively Nullified This Court's Prior Ruling 19

B. The District Court's Misapplication of Section 1806(f) Ensures That No One Can Watch the Watchman 24

CONCLUSION 28

TABLE OF AUTHORITIES

Page(s)

CASES

ACLU Found. of S. Cal. v. Barr,
952 F.2d 457 (D.C. Cir. 1991).....12

Bell Atl. Corp. v. Twombly,
550 U.S. 544 (2007).....22

City of Milwaukee v. Illinois,
451 U.S. 304 (1981).....13

El-Masri v. United States,
479 F.3d 296 (4th Cir. 2007).....15

Fazaga v. FBI,
916 F.3d 1202 (9th Cir. 2019).....*passim*

Gen. Dynamics Corp. v. United States,
563 U.S. 478 (2011).....15

In re NSA Telecomms Records Litig.,
595 F. Supp. 2d 1077 (N.D. Cal. 2009).....21, 22

Jewel v. NSA,
965 F. Supp. 2d 1090 (N.D. Cal. 2013).....10, 16

Kasza v. Browner,
133 F.3d 1159 (9th Cir. 1998).....15

Lexecon Inc. v. Milberg Weiss Bershad Hynes & Lerach,
523 U.S. 26 (1998).....12

Mayfield v. Gonzales,
2005 WL 1801679 (D. Or. July 28, 2005).....26

PLIVA, Inc. v. Mensing,
564 U.S. 604 (2011).....13

United States v. Hamidullin,
888 F.3d 62 (4th Cir. 2018).....13

Wikimedia Found. v. NSA/Cent. Sec. Serv.,
427 F. Supp. 3d 582 (D. Md. 2019).....18, 20, 21

Wikimedia Found. v. NSA/Cent. Sec. Serv.,
857 F.3d 193 (4th Cir. 2017).....19

CONSTITUTIONAL PROVISIONS

U.S. Const. amend. I. 19

U.S. Const. amend. IV. 19

STATUTES

50 U.S.C. § 1801(k) 4, 19

50 U.S.C. § 1802.....10

50 U.S.C. § 1803.....10

50 U.S.C. § 1804.....10

50 U.S.C. § 1805.....10

50 U.S.C. § 1806(c) 10, 11, 24, 25

50 U.S.C. § 1806(d) 10, 11, 24

50 U.S.C. § 1806(e) 10, 11, 24

50 U.S.C. § 1806(f).....*passim*

50 U.S.C. § 1809(a)(1).....9

50 U.S.C. § 1810.....9

50 U.S.C. § 1812.....9

RULES

Fed. R. App. P. 29(a) 2

Fed. R. Civ. P. 8 22

LEGISLATIVE MATERIALS

Hearing Before the S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, 94th Cong. (1975), https://www.intelligence.senate.gov/sites/default/files/94intelligence_activities_V.pdf 8

H.R. Rep. No. 95-1720 (1978) 12

S. Rep. No. 95-604 (1978) 12, 18, 24

S. Rep. No. 95-701 (1978) 10, 11, 12

Senate Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, Book II, S. Rep. No. 94-755 (1976), https://www.intelligence.senate.gov/sites/default/files/94755_II.pdf 8, 9, 17, 23

LITIGATION DOCUMENTS

Brief of Amici Curiae Professor Erwin Chemerinsky et al., *Hepting v. AT&T Corp.*, No. 06-17132 (9th Cir. May 2, 2007), Dkt. No. 37 1

Brief of Professors of Constitutional Law, Federal Jurisdiction, and Foreign Relations Law, *Mohamed v. Jeppesen Dataplan, Inc.*, No. 08-15693 (9th Cir. July 17, 2008), 2008 WL 6042363 1

Gov't's Supplemental FISA Notification, *United States v. Mohamud* No. 3:10-CR-00475-KI (D. Or. Nov. 19, 2013) 25

Hr'g Tr., *Jewel v. NSA,* No. 08-cv-04373 (N.D. Cal. May 19, 2017), ECF No. 362 21

MISCELLANEOUS

Trevor Aaronson, *NSA Secretly Helped Convict Defendants in U.S. Courts, Classified Documents Reveal*, The Intercept (Nov. 30, 2017), https://theintercept.com/2017/11/30/nsa-surveillance-fisa-section-702/ 25

Department of Justice, Office of Inspector General, *A Review of the FBI's Handling of the Brandon Mayfield Case* (2006), https://oig.justice.gov/special/s0601/final.pdf.....27

Department of Justice, Office of Inspector General, *Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation* (2019), https://www.justice.gov/storage/120919-examination.pdf.....26

European Commission: Staff Working Document, First Annual Review of the Privacy Shield (Oct. 18, 2017), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017SC0344 28

Philip Ewing, *What You Need to Know About the Much-Discussed Carter Page FISA Document*, NPR (July 23, 2018), https://www.npr.org/2018/07/23/631343524/what-you-need-to-know-about-the-much-discussed-carter-page-fisa-document 26

Elizabeth Goitein, *The FISA Court's 702 Opinions, Part I: A History of Non-Compliance Repeats Itself*, Just Security (Oct. 15, 2019), https://www.justsecurity.org/66595/the-fisa-courts-702-opinions-part-i-a-history-of-non-compliance-repeats-itself/.....27

Seymour M. Hersh, *Huge C.I.A. Operation Reported in U.S. Against Antiwar Forces, Other Dissidents in Nixon Years*, N.Y. Times, Dec. 22, 1974.....7

Loch K. Johnson, *Congress and the American Experiment in Holding Intelligence Agencies Accountable*, 28 J. Pol'y Hist. 494 (2016).....8

Dan Novack, *DOJ Still Ducking Scrutiny After Misleading Supreme Court on Surveillance*, The Intercept (Feb. 26, 2014), https://theintercept.com/2014/02/26/doj-still-ducking-scrutiny/.....25

Julian Sanchez, *Government Discretion in the Age of Bulk Data Collection: An Inadequate Limitation?*, 2 Harv. J. L. & Pub. Pol'y Federalist Ed. 23 (2014), https://www.harvard-jlpp.com/wp-content/uploads/sites/21/2015/02/Sanchez_Final-1.pdf.....8

Patrick C. Toomey, *Why Aren't Criminal Defendants Getting Notice of Section 702 Surveillance — Again?*, Just Security (Dec. 11, 2015), https://www.justsecurity.org/28256/arent-criminal-defendants-notice-section-702-surveillance-again/.....25

Stephen I. Vladeck, *The FISA Court and Article III*, 72 Wash. & Lee L. Rev. 1161 (2015).....25

Stephen I. Vladeck, *Standing and Secret Surveillance*, 9 ISJLP 552 (2014).....1

STATEMENT OF IDENTIFICATION

Amicus curiae Stephen I. Vladeck is the A. Dalton Cross Professor in Law at the University of Texas School of Law and a nationally recognized expert in the fields of national security, separation of powers, and surveillance law, including the Foreign Intelligence Surveillance Act ("FISA"). Professor Vladeck is the co-author of the *National Security Law* and *Counterterrorism Law* casebooks, a Distinguished Scholar at the Robert Strauss Center for International Security and Law, and the former Co-Editor-In-Chief of Just Security (https://www.justsecurity.org). He has also testified before the House Permanent Select Committee on Intelligence regarding potential amendments to FISA.

Professor Vladeck has a longstanding scholarly and jurisprudential interest in the proper interpretation and application of FISA, including its relationship to the state secrets privilege. Professor Vladeck has written extensively on these topics, authoring numerous amicus briefs and works of scholarship on FISA and the proper application of the state secrets privilege. *See, e.g.*, Brief of Professors of Constitutional Law, Federal Jurisdiction, and Foreign Relations Law, *Mohamed v. Jeppesen Dataplan, Inc.*, No. 08-15693 (9th Cir. July 17, 2008), 2008 WL 6042363; Brief of Amici Curiae Professor Erwin Chemerinsky et al., *Hepting v. AT&T Corp.*, No. 06-17132 (9th Cir. May 2, 2007), Dkt. No. 37; Stephen I. Vladeck, *Standing*

and Secret Surveillance, 9 ISJLP 552 (2014). He also joined the Brief of Law Professors as Amici Curiae in the prior appeal in this action.

Professor Vladeck is concerned that the District Court's ruling on remand disregards the careful balance that Congress enshrined in FISA between protecting state secrets and ensuring judicial review of genuine cases or controversies. Professor Vladeck submits this amicus brief in support of Appellant to explain how the District Court misapplied FISA, gave an undue role to the state secrets privilege, and eroded the separation of powers by disregarding the vital role that Congress assigned to the Judiciary in cases such as this.

All parties have consented to the filing of this brief pursuant to Fed. R. App. P. 29(a).[1]

[1] No party's counsel authored this brief in whole or in part. No party or party's counsel contributed money that was intended to fund preparation or submission of this brief. No person other than amicus or his counsel contributed money intended to fund the preparation or submission of this brief.

INTRODUCTION

In this case, the Wikimedia Foundation ("Wikimedia") challenges the constitutionality of the National Security Agency's ("NSA") "Upstream" internet surveillance program. This Court has already held that Wikimedia has standing to bring this suit because Wikimedia plausibly alleged that its communications were intercepted by the NSA. Nevertheless, on remand, the District Court held that Wikimedia was not an "aggrieved" party, and thus could not avail itself of the *in camera* review procedure that Congress created for cases like this. On that basis, the District Court found that the common-law state secrets privilege trumped the specific FISA provision that balances the protection of classified information with the ability of those harmed by NSA surveillance to vindicate their rights in court. These holdings were wrong, they were out of step with an on-point decision from the Ninth Circuit, and they should be reversed by this Court.

SUMMARY OF ARGUMENT

When Congress enacted FISA in 1978, it created special discovery procedures in order to ensure that parties challenging the legality of foreign intelligence surveillance could obtain meaningful judicial review. Those procedures authorize *ex parte in camera* review of "materials relating to electronic surveillance" "whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States." 50 U.S.C. § 1806(f). Wikimedia was fully entitled to

avail itself of this mechanism here: it plausibly alleged that it was an "aggrieved person" (someone "whose communications or activities were subject to electronic surveillance" (50 U.S.C. § 1801(k)); it made an appropriate "motion or request" to "discover or obtain applications or orders or other materials relating to electronic surveillance" (§ 1806(f)); and it asked the court to "determine whether the surveillance of the aggrieved person was lawfully authorized and conducted" (*id.*).

Nevertheless, on remand from this Court's decision finding that Wikimedia had standing to pursue its claims, the District Court refused to apply Section 1806(f). The District Court held that the state secrets privilege—rather than FISA's specialized *in camera* review mechanism—controlled. In so holding, the court made it impossible for Wikimedia to prove an essential element of its claim: that its communications were in fact intercepted or collected via the Upstream surveillance program. That ruling neutered Section 1806(f), upsetting the delicate balance of legislative, executive, and judicial power contemplated by FISA and allowing the common-law state secrets privilege to exceed its proper bounds. That decision should be reversed.

Amicus makes two central arguments in support of that result. *First*, Section 1806(f) was intended to apply—and to displace the state secrets privilege—in cases like this one. That is clear from the statute's text and from its legislative history, which shows that Congress wanted to curb unchecked intelligence surveillance by

the executive branch and to carefully balance the government's national security interests against individuals' civil liberties. Section 1806(f)'s *in camera* review procedure was a vital part of that effort. That procedure is mandatory, not precatory, and it applies broadly to *any* motion or request seeking discovery of information derived from electronic surveillance under FISA. The whole point of this provision was to ensure meaningful judicial oversight of electronic surveillance by ensuring that the government could not invoke secrecy to shut down court challenges to its surveillance activities. By establishing procedures for courts to receive and handle classified material when considering such challenges, Section 1806(f) replaced the common-law state secrets privilege with a mechanism that better balances the various interests at stake. This Court need not break new ground to reach that result: the Ninth Circuit's decision in *Fazaga v. FBI*, 916 F.3d 1202 (9th Cir. 2019), is directly on point in explaining why FISA's *in camera* review mechanism—not the state secrets privilege—governs cases like this.

Second, based on this Court's holding that Wikimedia properly alleged standing to challenge the NSA's surveillance, Wikimedia is an "aggrieved person" under Section 1806(f), and thus can invoke Section 1806(f)'s *in camera* review procedure. That follows both from prior case law and from basic rules of civil procedure, which make clear that plausible allegations unlock the gates to discovery. A discovery provision like Section 1806(f) cannot be withheld because a party lacks

admissible evidence—the whole point of such a provision is to allow that evidence to be uncovered.

The District Court's contrary conclusion turns Congress's carefully designed mechanism for ensuring a judicial check on surveillance abuses into an absurd Catch-22: only those able to prove that their communications were intercepted can use the provision; but only those who can use the provision are able to prove that their communications were intercepted. That is not the result FISA intended, and it effectively nullifies this Court's previous holding that Wikimedia has standing to pursue its claims. It makes no sense to hold that Wikimedia pleaded enough to get to discovery, but is forbidden from using the discovery mechanism Congress specifically provided for cases like this. That result also drains Section 1806(f) of nearly all of its force, transforming a mandatory provision into one that effectively operates at the election of the Executive and allowing the government to insulate its surveillance activities from legal challenges by anyone other than those whom it chooses to disclose that it surveilled.

This Court should reverse the District Court's decision, make clear that Section 1806(f) (rather than the common-law state secrets privilege) governs discovery, and allow Wikimedia's challenge to go forward.

ARGUMENT

I. FISA DISPLACES THE STATE SECRETS PRIVILEGE

In applying the state secrets privilege, rather than allowing Wikimedia to use the procedures established by Section 1806(f), the District Court disregarded both proper statutory interpretation and fundamental separation of powers principles. FISA's history, text, and structure—faithfully applied in the Ninth Circuit's on-point decision in *Fazaga*—all make clear that Section 1806(f) applies here and displaces the common-law state secrets privilege.

A. FISA, Including Section 1806(f), Was Enacted to Facilitate Judicial Oversight of Foreign Intelligence Surveillance

FISA "creates a comprehensive, detailed program to regulate foreign intelligence surveillance in the domestic context." *Fazaga*, 916 F.3d at 1232. Congress enacted the statute in 1978 in the wake of the Watergate scandal and outrage over the revelations that the executive branch had long been engaged in unauthorized domestic surveillance under the guise of national security. Following news reports that the CIA had unlawfully spied on Americans for decades, Congress established several special bipartisan committees to investigate the misconduct.[2] The most prominent of these was the Church Committee, chaired by Senator Frank

[2] *See e.g.*, Seymour M. Hersh, *Huge C.I.A. Operation Reported in U.S. Against Antiwar Forces, Other Dissidents in Nixon Years*, N.Y. Times, Dec. 22, 1974, at 1.

Church.[3] The Church Committee's comprehensive report revealed that "intelligence agencies [had] frequently wiretapped and bugged American citizens without the benefit of judicial warrant" and had "violated specific statutory provisions and infringed the constitutional rights of American citizens."[4] Among the abuses uncovered by the Church Committee was Project SHAMROCK, a program through which the NSA engaged in blanket surveillance of nearly all international telegram traffic that went through three major providers: "For almost 30 years, copies of most international telegrams originating in or forwarded through the United States were turned over to the National Security Agency and its predecessor agencies."[5] The NSA then used specific terms (names on a Watch List) to pare down the bulk data for analysis.[6]

---

[3] *See generally* Loch K. Johnson, *Congress and the American Experiment in Holding Intelligence Agencies Accountable*, 28 J. Pol'y Hist. 494, 498-99 (2016).

[4] *See* Senate Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, Book II, S. Rep. No. 94-755, at 12, 137 (1976) ("Church Committee Report"), https://www.intelligence.senate.gov/sites/default/files/94755_II.pdf.

[5] Hearing Before the S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, 94th Cong. 57-58 (1975), https://www.intelligence.senate.gov/sites/default/files/94intelligence_activities_V.pdf.

[6] *See* Julian Sanchez, *Government Discretion in the Age of Bulk Data Collection: An Inadequate Limitation?*, 2 Harv. J. L. & Pub. Pol'y Federalist Ed. 23, 24-25 (2014), https://www.harvard-jlpp.com/wp-content/uploads/sites/21/2015/02/Sanchez_Final-1.pdf.

FISA arose out of the Church Committee's recommendations. The Committee was especially concerned with the lack of any oversight for these surveillance activities, recognizing that the darkness in which the agencies operated encouraged abuse: "Knowledge is the key to control. Secrecy should no longer be allowed to shield the existence of constitutional, legal and moral problems from the scrutiny of … the American people themselves."[7] Among the Church Committee's recommendations was the creation of an expanded private right of action, in which "courts will be able to fashion discovery procedures, including inspection of material in chambers … to allow *plaintiffs* with *substantial claims* to uncover enough factual material to argue their case."[8]

Congress responded to these concerns in enacting FISA. The statute "sets out in detail roles for all three branches of government, providing judicial and congressional oversight of the covert surveillance activities by the executive branch combined with measures to safeguard secrecy necessary to protect national security." *Fazaga*, 916 F.3d at 1232. FISA expressly prohibits electronic surveillance "under color of law" except as statutorily authorized (50 U.S.C. §§ 1809(a)(1), 1812) and creates a private right of action that allows "aggrieved persons" subject to unauthorized electronic surveillance to sue for damages (§ 1810).

[7] Church Committee Report at 292.

[8] *Id.* at 337 (emphases added).

It also created a mechanism for a specialized court (the Foreign Intelligence Surveillance Court) to review and approve electronic surveillance requests made by the government. (§§ 1802-1805).

These provisions were all designed to impose a meaningful check on abusive surveillance activities—to allow the government to protect national security while ensuring that surveillance would be subject to judicial supervision that could curb abusive or illegal surveillance.[9]

Section 1806(f) was an integral part of this reform effort. This provision creates a mechanism for *in camera* review of information relating to electronic surveillance in all cases involving legal challenges to such surveillance:

> Whenever a court or other authority is notified pursuant to subsection (c) or (d), or whenever a motion is made pursuant to subsection (e), ***or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States*** or any State before any court or other authority of the United States or any State ***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 under this chapter, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, ***shall, notwithstanding any other law***, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United

[9] *See* S. Rep. No. 95-701, at 16 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 3985 (FISA was enacted to "reconcile national intelligence and counterintelligence needs with constitutional principals in a way that is consistent with both national security and individual rights"); *accord Fazaga*, 916 F.3d at 1233-34; *Jewel v. NSA*, 965 F. Supp. 2d 1090, 1104-05 (N.D. Cal. 2013).

> States, ***review in camera and ex parte*** the application, order, and such other materials relating to the surveillance as may be necessary ***to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted.***

50 U.S.C. § 1806(f) (emphases added). In crafting this provision, Congress adopted the Church Committee's recommendation regarding *in camera* discovery. The provision ensures that the government may continue to protect classified information that implicates national security while enabling effective judicial oversight of electronic surveillance activities.[10]

Two points about this provision bear emphasis here. *First*, Section 1806(f) applies extremely broadly: it is expressly *not* limited to cases where the government seeks to use information relating to electronic surveillance (under § 1806(c) and (d)) or to criminal cases in which a defendant seeks to suppress evidence (under §1806(e)). Instead, the statute also applies to "*any* motion or request" under "*any* statute or rule of the United States" to "discover" "materials relating to electronic surveillance." That readily includes civil actions like this one, in which a party seeks discovery relating to electronic surveillance in order to have the court determine whether that surveillance was "lawfully authorized and conducted."[11] The legislative

[10] *See* S. Rep. No. 95-701, at 64 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4032-33 ("[Section 1806(f) is] a reasonable balance between an entirely *in camera* proceeding … and mandatory disclosure.").

[11] The phrase "lawfully authorized and conducted" also plainly sweeps in not just questions of whether the surveillance was consistent with FISA itself, but also claims

history confirms this: the Senate "wishe[d] to make very clear that the procedures set out in [Section 1806(f)] apply whatever the underlying rule or statute referred to in [a party's] motion. This is necessary to prevent the carefully drawn procedures in [Section 1806(f)] from being bypassed by the inventive litigant using a new statute, rule or judicial construction."[12]

Second, Section 1806(f) is mandatory; it expressly displaces any other potentially applicable legal rule. The statute provides that courts "shall, notwithstanding any other law," conduct *in camera* review of surveillance materials. This language makes clear that, in the broad category of scenarios where the provision applies, courts ***must*** apply it. *Accord Lexecon Inc. v. Milberg Weiss Bershad Hynes & Lerach*, 523 U.S. 26, 35 (1998) (explaining that the "mandatory 'shall' … normally creates an obligation impervious to judicial discretion"). Not

---

that the surveillance, even if authorized by FISA, was unconstitutional. *See ACLU Found. of S. Cal. v. Barr*, 952 F.2d 457, 465 (D.C. Cir. 1991) ("When a district court conducts a § 1806(f) review, its task is not simply to decide whether the surveillance complied with FISA. Section 1806(f) requires the court to decide whether the surveillance was 'lawfully authorized and conducted.' The Constitution is law."); *accord* S. Rep. No. 95-701, at 63 (1978) (explaining that Section 1806(f)'s procedures would be employed to "determine whether the surveillance was authorized and conducted in a manner which did not violate *any constitutional or statutory right*" (emphasis added)).

[12] S. Rep. No. 95-604, pt. 1, at 57 (1978); *see also* H.R. Rep. No. 95-1720, at 31-32 (1978), *reprinted in* 1978 U.S.C.C.A.N. 4048, 4061 (explaining that Section 1806(f) applies "in both criminal and civil cases").

only that, they must do so ***in lieu of*** any other statute or common-law rule that might otherwise limit courts' ability to review classified material relating to electronic surveillance. *Accord PLIVA, Inc. v. Mensing*, 564 U.S. 604, 622 (2011) (explaining that a "non obstante provision in a new statute acknowledged that the statute might contradict prior law and instructed courts not to apply the general presumption against implied repeals").

In short, consistent with the overall regime established by FISA, Section 1806(f) creates mandatory, broadly applicable procedures that exclusively govern any situation where a party aggrieved by electronic surveillance seeks to discover classified information in order to challenge the legality of that surveillance.

B. As the Ninth Circuit Held in *Fazaga*, Section 1806(f) Displaces the State Secrets Privilege

This carefully designed legislative scheme leaves no room for the state secrets privilege. "[A] statute preempts common law when Congress speaks directly to the question." *United States v. Hamidullin*, 888 F.3d 62, 75 (4th Cir. 2018); *accord City of Milwaukee v. Illinois*, 451 U.S. 304, 313-15 (1981) ("We have always recognized that federal common law is subject to the paramount authority of Congress. It is resorted to [i]n absence of an applicable Act of Congress."). That is precisely what Congress has done here. As discussed above, the text of Section 1806(f), supported by its legislative history and purpose, shows a clear intent to regulate discovery of information related to electronic surveillance, without regard for a common-law

privilege that might otherwise restrict the ability of parties challenging unlawful surveillance to prove their claims.

This Court need not break any new ground to reach that conclusion. Just last year, in *Fazaga*, the Ninth Circuit addressed this same issue and held that "in enacting FISA, Congress displaced the common-law dismissal remedy created by the *Reynolds* state secrets privilege as applied to electronic surveillance within FISA's purview." 916 F.3d at 1230. *Fazaga* was a putative class action by three plaintiffs who alleged that the FBI had conducted an unlawful covert surveillance program to gather information about Muslims based on their religious identity. Plaintiffs brought civil claims seeking damages for various constitutional and statutory violations. In response, the government invoked the state secrets privilege to block certain kinds of evidence from discovery and to seek dismissal of some of plaintiffs' claims. The district court dismissed all but one of the claims based on the privilege. The Ninth Circuit reversed, holding that the district court should instead "have relied on FISA's alternative procedures for handling sensitive national security information." *Id*. at 1225.

In addressing that issue, the Ninth Circuit explained that the initial question was "whether the procedures established under FISA for adjudicating the legality of challenged electronic surveillance replace the common law state secrets privilege with respect to such surveillance to the extent that privilege allows the categorical

dismissal of causes of action." *Id*. at 1226. This was a matter of statutory interpretation: because the state secrets privilege is federal common law, "the relevant inquiry in deciding if a statute preempts the state secrets privilege is whether the statute 'speaks directly to the question otherwise answered by federal common law.'" *Id*. at 1230-31 (explaining that the "state secrets privilege may have 'a constitutional core or constitutional overtones,' but, at bottom, it is an evidentiary rule rooted in common law, not constitutional law" (quoting *Kasza v. Browner*, 133 F.3d 1159, 1167 (9th Cir. 1998))); *accord Gen. Dynamics Corp. v. United States*, 563 U.S. 478, 485 (2011) (describing the state secrets privilege as an "evidentiary rule[]").[13]

And, as the Ninth Circuit observed, "the text of FISA does speak quite directly to the question otherwise answered by the dismissal remedy sometimes required by the common law state secrets privilege." *Fazaga*, 916 F.3d at 1231. Section 1806(f) creates a "mandatory procedure," which "necessarily overrides, on the one hand, the usual procedural rules precluding such severe compromises of the adversary process

[13] As the Ninth Circuit noted, this Court, in *El-Masri v. United States*, 479 F.3d 296, 303-04 (4th Cir. 2007), discussed "the constitutional significance of the state secrets privilege, while recognizing its common law roots." *Fazaga*, 916 F.3d at 1230. Nothing in *El-Masri* suggests that Congress cannot displace the state secrets privilege through a statute that creates an alternative procedure, nor does *El-Masri* "specify a clear statement rule" for Congress to do so. *Id*. *El-Masri* simply did not address the issues raised by *Fazaga*—or by this case.

and, on the other, the state secrets evidentiary dismissal option." *Id*. at 1231-32. Indeed, the procedures created by Section 1806(f) "are animated by the same concerns" that underlie the privilege and are triggered by a virtually identical process (an affidavit from the Attorney General). *Id*. at 1232. "In this sense, § 1806(f) 'is, in effect, a codification of the state secrets privilege for purposes of relevant cases under FISA, as modified to reflect Congress's precise directive to the federal courts for the handling of electronic surveillance materials and information with purported national security implications.'" *Id*. (quoting *Jewel v. NSA*, 965 F. Supp. 2d 1090, 1106 (N.D. Cal. 2013)).

"In short," the Ninth Circuit concluded, the procedures set out in Section 1806(f) "constitute 'Congress's specific and detailed description for how courts should handle claims by the government that the disclosure of material relating to or derived from electronic surveillance would harm national security.'" *Id*. at 1234 (quoting *Jewel*, 965 F. Supp. 2d at 1106). Where those procedures apply, they leave no room for the state secrets privilege. *Id*.

And, as discussed above, Section 1806(f) applies broadly. *Fazaga* squarely rejected the government's argument that the procedures of 1806(f) "do not apply to any affirmative claims challenging the legality of electronic surveillance or the use of information derived from electronic surveillance." *Id*. at 1235-38. The court correctly recognized that this argument was directly contrary to the "plain text and

statutory structure of FISA." *Id.* at 1235. And it had little trouble concluding that "FISA's § 1806(f) procedures are to be used when an aggrieved person affirmatively challenges, in any civil case, the legality of electronic surveillance or its use in litigation, whether the challenge is under FISA itself, the Constitution, or any other law." *Id.* at 1238.

This court should follow *Fazaga*. The Ninth Circuit's decision is scholarly, thorough, and wholly consistent with FISA's text, purpose, and legislative history. Under *Fazaga*, and based on the plain language of FISA, the procedures set forth in Section 1806(f) displace the state secrets privilege in cases like this, which challenge the legality of electronic surveillance. Those procedures foreclose the government from relying on that privilege either to avoid producing relevant materials for *ex parte in camera* review or to obtain dismissal of a plaintiff's claim because it implicates "state secrets." Any other result undermines the core principles animating FISA, which was enacted because of revelations that the government had been defying legal rules and compromising the personal liberties of Americans in the process.[14] If the government can sidestep Section 1806(f) by invoking the state secrets privilege, the government effectively has the right to choose whether to opt

[14] *See, e.g.*, Church Committee Report at 289 ("[I]ntelligence activities have undermined the constitutional rights of citizens and … have done so primarily because checks and balances designed by the framers of the Constitution to assure accountability have not been applied.").

into FISA, and the law's mandatory provisions become advisory. Allowing the government to avoid meaningful judicial review in this way would enable the Executive once again to "conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it"—exactly what FISA was intended to prevent.[15]

II. A PARTY WHO HAS ADEQUATELY ALLEGED STANDING TO CHALLENGE SURVEILLANCE ACTIVITY IS AN "AGGRIEVED PERSON" AUTHORIZED TO INVOKE THE *IN CAMERA* REVIEW PROCEDURE OF SECTION 1806(f)

The District Court's decision tried to sidestep all of this by finding that Wikimedia could not avail itself of Section 1806(f) because it could not "make a factual showing that Wikimedia was the subject of electronic surveillance using admissible record evidence," and, therefore, it was not an "aggrieved person" under FISA. *Wikimedia Found. v. NSA/Cent. Sec. Serv.*, 427 F. Supp. 3d 582, 614 (D. Md. 2019). This ruling is wrong: it misreads the statute, it is at odds with both *Fazaga* and this Court's prior decision in this case, and it undermines the basic purpose of Section 1806(f).

[15] S. Rep. No. 95-604, pt. 1, at 8, 1978 U.S.C.C.A.N. at 3910.

A. The District Court Misapplied FISA and Effectively Nullified This Court's Prior Ruling

In its previous decision in this case, this Court held that Wikimedia plausibly alleged standing to challenge the legality of the Upstream surveillance program. *Wikimedia Found. v. NSA/Cent. Sec. Serv.*, 857 F.3d 193, 209-11 (4th Cir. 2017). The Court found that Wikimedia had put forward specific, non-conclusory allegations that its communications were among the mass of internet communications intercepted by the government through the Upstream program. *Id*. Wikimedia pleaded "three key facts" that were "sufficient to make plausible the conclusion that the NSA is intercepting, copying, and reviewing at least some of Wikimedia's communications." *Id*. The Court concluded that these allegations established that Wikimedia suffered an "injury in fact" that was "concrete and particularized." *Id*. at 210; *see also id*. at 212 ("Wikimedia's detailed allegations suffice to plausibly establish cognizable injuries under the First and Fourth Amendments.").

As a matter of law, this conclusion was sufficient to make Wikimedia an "aggrieved person" under FISA. The statute defines "aggrieved person" as "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance." 50 U.S.C. § 1801(k). This is precisely what this Court held Wikimedia plausibly alleged. 857 F.3d at 209 ("[T]he Wikimedia Allegation is that the NSA is intercepting, copying,

and reviewing at least some of Wikimedia's communications in the course of Upstream surveillance."). Nothing more was required for Wikimedia to avail itself of Section 1806(f).

Once again, *Fazaga* is directly on point. There, the Ninth Circuit explained, the plaintiffs "allege in extensive detail in the complaint that they were subjected to many and varied instances of audio and video surveillance. The complaint's allegations are sufficient if proven to establish that Plaintiffs are 'aggrieved persons.'" *Fazaga*, 916 F.3d at 1216. Based on nothing more than those plausible allegations, the Ninth Circuit went on to hold that "because Plaintiffs are properly considered 'aggrieved' for purposes of FISA," the procedures of Section 1806(f) were "directly applicable." *Id*. at 1239.

In a strained attempt to distinguish *Fazaga*, the District Court tautologically characterized the Ninth Circuit's decision as holding that "§ 1806(f)'s procedures displace a dismissal remedy for the *Reynolds* state secrets doctrine only where § 1806(f)'s procedures apply." *Wikimedia Found.*, 427 F. Supp. 3d at 614. Obviously, Section 1806(f) applies only where it applies. But the District Court lost sight of the fact that the Ninth Circuit expressly held that the *Fazaga* plaintiffs were "aggrieved persons" eligible to use Section 1806(f) ***simply based on the allegations of their complaint***. The District Court suggested that the Ninth Circuit's decision "says nothing" about the relationship between Section 1806(f) and the state secrets

privilege where "a plaintiff has not established that he, she, or it is an 'aggrieved person' using admissible record evidence." 427 F. Supp. 3d at 614 n.60. But that just begs the question and assigns to the Ninth Circuit a wholly absurd outcome: in the District Court's view, Fazaga's allegations were enough to make him an "aggrieved person" (and thereby avoid dismissal on state secrets grounds) but not enough for him actually to use the procedure designed to enable aggrieved persons to discover information that could allow them to prove their case. That makes no sense, and it is plainly not what the Ninth Circuit contemplated. In holding that *Fazaga* plaintiffs were "aggrieved" based on their allegations, the Ninth Circuit held that Section 1806(f)'s discovery mechanism was open to them and the state secrets privilege did not apply. The District Court's decision to foreclose that mechanism cannot be squared with *Fazaga*, or with any sensible understanding of FISA.

The District Court's approach is similarly at odds with *In re NSA Telecommunications Records Litigation*, 595 F. Supp. 2d 1077, 1083 (N.D. Cal. 2009), which squarely rejected the argument that "only affirmative confirmation by the government or equally probative evidence will meet the 'aggrieved person' test." Instead, the *NSA* court explained that plaintiffs had "alleged enough to plead 'aggrieved person' status so as to proceed to the next step in proceedings under FISA's section 1806(f)." *Id.* at 1086; *see also* Hr'g Tr. 32:23-32:25, *Jewel v. NSA,* No. 08-cv-04373 (N.D. Cal. May 19, 2017), ECF No. 362 (ordering *in camera*

review under Section 1806(f) of evidence relevant to plaintiffs' standing where the government had not confirmed its surveillance). As the court explained, if "only affirmative confirmation by the government or equally probative evidence will meet the 'aggrieved person' test," it "would effectively render [that] provision[] of FISA without effect." *In re NSA Telecomms.*, 595 F. Supp. 2d at 1083, 1086.

These holdings reflect basic principles of civil procedure. A party need not prove its case with evidence to unlock the gates to discovery. The purpose of discovery is to uncover evidence. It is the allegations in a plaintiff's complaint that determine whether its claims can proceed. Wikimedia's plausible allegations that its communications had been collected through electronic surveillance allowed it to survive a motion to dismiss and proceed to discovery. *Accord Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 556 (2007) (Rule 8's pleading standard "calls for enough fact to raise a reasonable expectation that discovery will reveal evidence" that would allow a plaintiff to survive summary judgment).

The District Court's decision turned this fundamental procedure on its head. It means that FISA's discovery procedures are available only to those who already have definitive evidence that they were surveilled, even though such evidence is often only attainable through the procedures that the court ruled off limits. That result transforms Section 1806(f) into a Catch-22—a taunting illusion that offers the promise, but not the reality, of meaningful judicial review. This undermines a basic

aim of Section 1806(f): to enable "plaintiffs with substantial claims to uncover enough factual material to argue their case, while protecting the secrecy of governmental information in which there is a legitimate security interest."[16] In short, a plaintiff need not prove it was the target of electronic surveillance before availing itself of the mechanism that Congress specifically devised for obtaining such proof. Plausible allegations are enough.

In holding otherwise, the District Court did not merely misapply FISA, it also neutered this Court's holding that Wikimedia had alleged standing. The thrust of this Court's prior decision was that Wikimedia had alleged enough to establish that it was injured by the NSA's unlawful electronic surveillance. It makes no sense to say (as this Court did) that Wikimedia was entitled to pursue discovery because it plausibly pleaded that it was aggrieved, but (as the District Court did on remand) that Wikimedia is *not* entitled to meaningful discovery because it cannot yet prove that it was aggrieved. In finding that Wikimedia could survive a motion to dismiss, this Court determined that Wikimedia has a substantial claim of the sort envisioned by the Church Committee. But the District Court deprived Wikimedia of any effective ability to pursue that claim. That decision cannot be squared with the statute or this Court's ruling, and it should be reversed.

[16] Church Committee Report at 337.

B. The District Court's Misapplication of Section 1806(f) Ensures That No One Can Watch the Watchman

There is yet another problem with the District Court's approach. The argument that the court embraced—that Section 1806(f)'s procedures apply only to persons expressly notified by the government that they were the targets of foreign intelligence surveillance—would effectively give the government unilateral control over those procedures. It would allow the government to limit the application of Section 1806(f) to cases where it chooses to volunteer that a plaintiff has been surveilled. That, in turn, would negate FISA's animating purpose to "curb the practice by which the Executive Branch may conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it."[17]

Under the District Court's application of FISA, there would effectively be only two kinds of individuals who could use Section 1806(f)'s procedures: (1) criminal defendants against whom prosecutors seek to introduce evidence obtained from surveillance (50 U.S.C. § 1806(c)-(e)); and (2) individuals who learn about their surveillance through government admission (50 U.S.C. § 1806(f)). And both categories are much narrower than they first appear.

As for the first, the government has not provided and is not providing notice to all criminal defendants against whom FISA surveillance is being used:

[17] S. Rep. No. 95-604, pt. 1, at 8.

> [T]he government reportedly failed to satisfy its notice obligations under FISA for a substantial period of time, culminating in a rare public concession by Solicitor General Verrilli in October 2013 that a number of defendants had not received the notice required by FISA—and had therefore been unable to vindicate their right to collaterally attack the underlying FISA warrant.[18]

Despite this concession, the government has apparently continued not to make these disclosures. For instance, the government filed a "supplemental notice" in *United States v. Mohamud* explaining that it had "offered into evidence or otherwise used or disclosed …, in the above-captioned matter information derived from acquisition of foreign intelligence information conducted pursuant to" FISA.[19] But it filed that notice 10 months *after the defendant was already convicted*.[20] Numerous others have similarly reported that, even after Verrilli's apology, the Department of Justice's disclosure of FISA surveillance has been extremely limited.[21] Given the

---

[18] Stephen I. Vladeck, *The FISA Court and Article III*, 72 Wash. & Lee L. Rev. 1161, 1170 (2015); *see also* 50 U.S.C. § 1806(c).

[19] Gov't's Supplemental FISA Notification, No. 3:10-CR-00475-KI (D. Or. Nov. 19, 2013), ECF No. 486.

[20] *See* Dan Novack, *DOJ Still Ducking Scrutiny After Misleading Supreme Court on Surveillance*, The Intercept (Feb. 26, 2014), https://theintercept.com/2014/02/26/doj-still-ducking-scrutiny/.

[21] *See* Trevor Aaronson, *NSA Secretly Helped Convict Defendants in U.S. Courts, Classified Documents Reveal*, The Intercept (Nov. 30, 2017), https://theintercept.com/2017/11/30/nsa-surveillance-fisa-section-702/ (noting that "[t]he Intercept found . . . just 10 [terrorism criminal defendants] received notice of Section 702 surveillance," while, years earlier, the government reported that FISA surveillance resulted in "well over 100 arrests on terrorism-related offenses"); *accord* Patrick C. Toomey, *Why Aren't Criminal Defendants Getting Notice of*

government's consistent refusal to disclose its surveillance even of criminal defendants where legal mandates should apply, civil plaintiffs cannot expect notice from the government.

As to the second category, the District Court's approach would essentially limit Section 1806(f)'s application in civil cases to two plaintiffs: Carter Page and Brandon Mayfield. In Page's case, the FISA warrants were disclosed for highly political reasons in response to the investigation into the Trump campaign's ties to Russia.[22] In Mayfield's, the Government admitted that Mayfield was the target of FISA surveillance only after a disastrously bungled investigation. *See Mayfield v. Gonzales*, 2005 WL 1801679, at *17 (D. Or. July 28, 2005). Indeed, Mayfield's case in particular underscores how prone to abuse the FISA program is. Mayfield was electronically surveilled after the FBI incorrectly concluded that his fingerprints were on one of the detonators found near terrorist attacks in Madrid, Spain. The Department of Justice Inspector General determined that bias against Mayfield's

---

Section 702 Surveillance — Again?, Just Security (Dec. 11, 2015), https://www.justsecurity.org/28256/arent-criminal-defendants-notice-section-702-surveillance-again/ (no Section 702 notices issued between April 2014 and December 2015).

[22] Philip Ewing, *What You Need to Know About the Much-Discussed Carter Page FISA Document*, NPR (July 23, 2018), https://www.npr.org/2018/07/23/631343524/what-you-need-to-know-about-the-much-discussed-carter-page-fisa-document; Department of Justice, Office of Inspector General, *Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation* at xiii (2019), https://www.justice.gov/storage/120919-examination.pdf.

"Muslim religion" within the Department of Justice contributed to the FBI's refusal to reevaluate the false identification, which led to Mayfield's continued surveillance.[23]

Mayfield's case is consistent with the other reporting on malfeasance and mistakes in our nation's surveillance system.[24] And collectively, these consistent reports of surveillance abuse and the government's failure to report surveillance illustrate the danger inherent in the District Court's exceedingly narrow interpretation of "aggrieved person" under Section 1806(f). Indeed, to hold that the *in camera* review procedure is available only when the government has given its consent would strip the statute of any real force in checking abusive and illegal surveillance. It would transform a mandatory procedure into one that effectively operates at the election of the Executive.

While that result was championed by the government below, it contradicts the government's own representations to the European Union ("EU"). In 2017, as part

---

[23] *See* Department of Justice, Office of Inspector General, *A Review of the FBI's Handling of the Brandon Mayfield Case*, (2006) https://oig.justice.gov/special/s0601/final.pdf.

[24] *See, e.g.*, Elizabeth Goitein, *The FISA Court's 702 Opinions, Part I: A History of Non-Compliance Repeats Itself*, Just Security (Oct. 15, 2019), https://www.justsecurity.org/66595/the-fisa-courts-702-opinions-part-i-a-history-of-non-compliance-repeats-itself/ ("This is now the fourth major FISA Court opinion on Section 702 in 10 years documenting substantial non-compliance with the rules meant to protect Americans' privacy.").

of the debate over renewing the EU-US Privacy Shield—an agreement which allows for the transmission of EU data to the United States without added restrictions if the EU approves U.S. data safeguards—many questioned the adequacy of U.S. safeguards. Among other things, critics observed that individuals could not challenge U.S. surveillance under FISA. In response, and in defense of its data safeguards, the U.S. government pointed to this Court's holding in the prior appeal as proof that plaintiffs could proceed beyond the initial stages of litigation: "[T]he U.S. authorities have pointed the Commission to the proceedings in … *Wikimedia v. National Security Agency*[, which] suggest that, depending on the circumstances, applicants can succeed at the admissibility stage."[25] But, as explained above, the District Court's decision sapped that decision of any force. The Government should not be permitted to tout the benefits of judicial oversight of its surveillance powers only to negate them when the spotlight is off.

CONCLUSION

For these reasons, this Court should reverse the District Court's decision and remand this case with instruction to allow Wikimedia to use Section 1806(f) to conduct discovery.

[25] European Commission: Staff Working Document, First Annual Review of the Privacy Shield, at 33-34 (Oct. 18, 2017), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017SC0344.

July 8, 2020

Respectfully submitted,

WILSON SONSINI GOODRICH & ROSATI

By: */s/ Brian M. Willen*
Brian M. Willen

Attorney for Amicus
PROFESSOR STEPHEN I. VLADECK

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of Rule 29(a)(5) of the Federal Rules of Appellate Procedure. The brief contains 6,455 words, excluding the parts of the brief exempted by Rule 32(f).

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

July 8, 2020

WILSON SONSINI GOODRICH & ROSATI

By: */s/ Brian M. Willen*
Brian M. Willen

Attorney for Amicus
STEPHEN I. VLADECK