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

BRIEF FOR 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

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

DISCLOSURE STATEMENT

- In civil, agency, bankruptcy, and mandamus cases, a disclosure statement must be filed by **all** parties, with the following exceptions: (1) the United States is not required to file a disclosure statement; (2) an indigent party is not required to file a disclosure statement; and (3) a state or local government is not required to file a disclosure statement in pro se cases. (All parties to the action in the district court are considered parties to a mandamus case.)
- In criminal and post-conviction cases, a corporate defendant must file a disclosure statement.
- In criminal cases, the United States must file a disclosure statement if there was an organizational victim of the alleged criminal activity. (See question 7.)
- Any corporate amicus curiae must file a disclosure statement.
- Counsel has a continuing duty to update the disclosure statement.

No. 20-1191 Caption: Wikimedia Foundation v. National Security Agency, et al.

Pursuant to FRAP 26.1 and Local Rule 26.1,

Wikimedia Foundation
(name of party/amicus)

who is appellant, makes the following disclosure:
(appellant/appellee/petitioner/respondent/amicus/intervenor)

1. Is party/amicus a publicly held corporation or other publicly held entity? ☐YES ☑NO

2. Does party/amicus have any parent corporations? ☐YES ☑NO
If yes, identify all parent corporations, including all generations of parent corporations:

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? ☐YES ☑NO
If yes, identify all such owners:

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation? ☐YES ☑NO
If yes, identify entity and nature of interest:

5. Is party a trade association? (amici curiae do not complete this question) ☐YES ☑NO
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:

6. Does this case arise out of a bankruptcy proceeding? ☐YES ☑NO
If yes, the debtor, the trustee, or the appellant (if neither the debtor nor the trustee is a party) must list (1) the members of any creditors' committee, (2) each debtor (if not in the caption), and (3) if a debtor is a corporation, the parent corporation and any publicly held corporation that owns 10% or more of the stock of the debtor.

7. Is this a criminal case in which there was an organizational victim? ☐YES ☑NO
If yes, the United States, absent good cause shown, must list (1) each organizational victim of the criminal activity and (2) if an organizational victim is a corporation, the parent corporation and any publicly held corporation that owns 10% or more of the stock of victim, to the extent that information can be obtained through due diligence.

Signature: s/Patrick Toomey Date: July 1, 2020

Counsel for: Wikimedia Foundation

Print to PDF for Filing

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Other Authorities

STATEMENT OF JURISDICTION

The district court had jurisdiction pursuant to 28 U.S.C. § 1331. The court entered a final order granting Defendants' motion for summary judgment on December 16, 2019. JA.7: 4123. Plaintiff filed a notice of appeal on February 14, 2020. JA.7: 4124. This Court has jurisdiction pursuant to 28 U.S.C. § 1291.

STATEMENT OF THE ISSUES

1. Does Wikimedia's evidence, which shows that some of its trillions of communications are "virtually certain" to be subject to Upstream surveillance, establish a genuine dispute of material fact with respect to its standing?

2. Does the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1806(f)—which establishes mandatory procedures for in camera review of classified discovery in cases challenging FISA surveillance—displace the common-law state secrets privilege and require the district court to review any sensitive evidence in this case in camera?

3. Even if FISA's in camera review procedures do not apply here, do the government's official disclosures about the operation and breadth of Upstream surveillance foreclose its reliance on the state secrets privilege?

4. Does Wikimedia's evidence of lost readership, self-censorship, and mitigation measures provide an alternative basis on which a reasonable factfinder could rely to find standing?

5. Finally, if Wikimedia itself has standing, has it also presented sufficient evidence to support third-party standing to assert the privacy and expressive rights of its users?

STATEMENT OF THE CASE

I. Introduction

This lawsuit challenges the suspicionless seizure and searching of U.S. persons' international Internet communications by the National Security Agency ("NSA"). As the government's own disclosures make clear, the NSA is systematically searching through communications flowing into and out of the United States on the Internet's central arteries, looking for information relating to thousands of foreign-intelligence surveillance targets. This surveillance system, called "Upstream" surveillance, involves an unprecedented invasion of Americans' privacy. It is the digital analogue of having a government agent open every letter that comes through a mail processing center to examine its contents before determining which letters to keep. The Constitution has never permitted such indiscriminate searches of Americans' private communications, but the government—equipped with new technologies—claims that sweeping power here.

Although the NSA's mass surveillance of Americans' international communications raises grave constitutional questions, its lawfulness has yet to be considered by any ordinary court. The Wikimedia Foundation—which operates the

online encyclopedia Wikipedia—brought suit to challenge the constitutionality of Upstream surveillance. This surveillance violates the First and Fourth Amendments because it involves warrantless and suspicionless surveillance of Americans' communications en masse. It also violates Article III because it is predicated upon mass surveillance orders issued by the Foreign Intelligence Surveillance Court ("FISC") in the absence of any case or controversy.

In the five years since Wikimedia filed this suit, however, the government has yet to defend the lawfulness of Upstream surveillance. Instead, it has challenged Wikimedia's standing. This Court previously rejected the government's motion to dismiss the suit based on standing, holding that Wikimedia had plausibly alleged that the NSA was surveilling its communications. Wikimedia has now substantiated its core standing allegations with an extensive record of government disclosures about the operation of Upstream surveillance, and with detailed expert declarations explaining that—due to the volume and global distribution of Wikimedia's trillions of Internet communications, and due to the way in which Upstream surveillance operates—it is "virtually certain" that the NSA has copied and reviewed Wikimedia's communications and that it continues to do so. In holding that this evidence did not show a genuine dispute of material fact, the district court repeatedly erred: it failed to credit Wikimedia's evidence as true; it drew inferences against Wikimedia; and it inverted the parties' burdens at

summary judgment.

The district court also erred in failing to follow the mandatory procedures that Congress has put in place to protect sensitive information while allowing civil challenges to FISA surveillance to proceed. *See* 50 U.S.C. § 1806(f). These procedures require in camera review in cases like this one, so that unilateral assertions of executive secrecy do not thwart the judicial oversight that Congress deemed essential to preventing overreaching government surveillance. The government claims that allowing this case to proceed would reveal state secrets, entitling it to dismissal. But FISA's procedures displace the common-law state secrets privilege here, and they reflect Congress's careful balancing of competing interests. The district court was bound to apply these procedures to review the actual evidence, rather than dismissing the case on the government's say-so.

Moreover, even if FISA's procedures did not apply, litigation of this case would not endanger state secrets. As this Court has already recognized, Wikimedia is no ordinary plaintiff. *See Wikimedia Found. v. NSA*, 857 F.3d 193, 200 (4th Cir. 2017). Due to the incredible volume of its communications and the global distribution of its users, Wikimedia's communications are ubiquitous, and so permitting this litigation to go forward would not reveal any sensitive facts about Upstream surveillance beyond those the government itself has already disclosed.

For these reasons, explained more fully below, this case should proceed

using the procedures that Congress mandated in FISA.

II. Statutory Background

A. The Foreign Intelligence Surveillance Act of 1978

In 1975, Congress established a committee, chaired by Senator Frank Church, to investigate allegations of "substantial wrongdoing" by the intelligence agencies in their conduct of surveillance. Final Report of the S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities (Book II), S. Rep. No. 94-755, at v (1976). The Committee discovered that, over decades, the intelligence agencies had "infringed the constitutional rights of American citizens" and "intentionally disregarded" limitations on surveillance in the name of "national security." *Id.* at 137. Of particular concern was that the agencies had "pursued a 'vacuum cleaner' approach to intelligence collection," in some cases intercepting Americans' communications under the pretext of targeting foreigners. *Id.* at 165. In response, the Committee recommended that all surveillance of communications "to, from, or about an American without his consent" be subject to a warrant procedure. *Id.* at 309.

In 1978, in response, Congress enacted FISA to regulate surveillance conducted for foreign intelligence purposes. The statute created the FISC and empowered it to review government applications for surveillance in certain foreign intelligence investigations. 50 U.S.C. § 1803(a). As originally enacted, FISA

generally required the government to obtain an individualized order from the FISC—based on a detailed factual showing—before conducting electronic surveillance on U.S. soil. *Id.* §§ 1804(a), 1805. The FISC could issue an order authorizing surveillance only if it found that, among other things, there was "probable cause to believe that the target of the electronic surveillance [was] a foreign power or an agent of a foreign power." *Id.* § 1805(a)(2).

The basic framework established by FISA remains in effect today, but it has been severely weakened by Section 702, as described below.

B. Warrantless Surveillance Under Section 702

Section 702 of FISA was enacted in 2008, and radically revised the FISA regime by authorizing the warrantless acquisition of U.S. persons' international communications from companies inside the United States. Surveillance under Section 702 is far more sweeping than surveillance traditionally conducted under FISA.[1]

First, Section 702 allows the surveillance of U.S. persons' international communications without a warrant or any individualized court approval. Instead, the FISC's role consists principally of reviewing, on an annual basis, the general procedures the government proposes to use in carrying out its surveillance. 50

[1] Wikimedia uses the phrase "U.S. persons" to refer to U.S. citizens and residents. Wikimedia uses the term "international" to describe communications that either originate or terminate outside the United States, but not both.

U.S.C. § 1881a(j).

Second, Section 702 authorizes surveillance not predicated on probable cause or on any suspicion of wrongdoing. The statute permits the government to target *any* foreigner located outside the United States to obtain "foreign intelligence information"—which is defined broadly to include any information bearing on the foreign affairs of the United States. *Id.* §§ 1881a(a), 1801(e). The government's targets need not be agents of foreign powers, terrorists, or connected even remotely with criminal activity.

In short, Section 702 exposes every international communication—that is, every communication between an individual in the United States and a non-American abroad—to potential surveillance. As discussed below, the government is using the statute to conduct precisely the kind of vacuum-cleaner-style surveillance that the Church Committee condemned and that the Fourth Amendment was intended to prohibit.

III. Statement of the Facts

A. Wikimedia, Its Global User Community, and Its Communications

As the operator of one of the most-visited websites in the world, Wikimedia engages in more than one trillion international Internet communications each year. JA.3: 2255, 2264. Wikimedia communicates with hundreds of millions of people in every country on earth—as they read, edit, and contribute to the twelve

Wikimedia "Projects." JA.3: 2264, 2220-21.[2] The best-known of Wikimedia's Projects is Wikipedia, a free Internet encyclopedia that is one of the largest collections of shared knowledge in human history.

Wikimedia's communications are essential to its organizational mission, as is its ability to protect the privacy of these communications. JA.3: 2235, 2242. Wikimedia's international Internet communications include communications with Wikimedia community members as they read, edit, and contribute to this vast repository of human knowledge; internal "log" communications; and staff communications. JA.3: 2223-31.

B. The Government's Implementation of Section 702

The government has implemented Section 702 broadly, relying on the statute to intercept and retain huge volumes of Americans' communications. Privacy & Civil Liberties Oversight Board ("PCLOB") Report 152 (JA.4: 2591). In 2011 alone, the government relied on Section 702 to intercept and retain more than 250 million communications—a number that does not reflect the far larger quantity of communications whose contents the NSA searched before discarding them. *Id.* at 37, 111 n.476, 116 (JA.4: 2476, 2550, 2555). Each year, the NSA targets more than 100,000 individuals and groups for surveillance under Section 702. JA.4:

[2] This includes communications between foreign users and Wikimedia's U.S.-based servers, and communications between U.S. users and Wikimedia's foreign servers. JA.3: 2265-66.

2762. Whenever a U.S. person communicates with any one of the government's targets, his or her communications can be intercepted and retained.

This case concerns Upstream surveillance, one of the forms of surveillance conducted under Section 702.

C. Upstream Surveillance

Upstream surveillance involves the government's warrantless search and seizure of U.S. persons' Internet communications on U.S. soil. PCLOB Report 36-41 (JA.4: 2475-80). To conduct this surveillance, the NSA copies and reviews the contents of Americans' communications as they flow across major Internet circuits, looking for thousands of search terms associated with its targets. *Id.*; 2d Bradner Decl. ¶¶ 13-16 (JA.7: 3887-88).

The government has disclosed a significant amount of information about Upstream surveillance, including dozens of FISC opinions and filings, an exhaustive report by the Privacy and Civil Liberties Oversight Board, public testimony by intelligence officials, and official statements by the NSA. *See, e.g.*, PCLOB Report (JA.4: 2436) (citing numerous official disclosures); ODNI Document Release (JA.4: 2718).

To conduct Upstream surveillance, the NSA intercepts communications that transit Internet "backbone" circuits—the "high-speed, ultra-high bandwidth" Internet circuits operated by major communication service providers. PCLOB

Report 36-37 (JA.4: 2475-76); JA.4: 2739. The NSA scans international Internet communications that transit these circuits to find "selectors"—such as email addresses or phone numbers—associated with its many targets. PCLOB Report 37-41 (JA.4: 2476-80); JA.4: 2729-30, 2737-38.

The breadth of Upstream surveillance is a function, in large part, of how communications traverse the Internet. When an individual engages in any kind of Internet activity, such as browsing a webpage or sending an email, her communications are broken up into data "packets"—small chunks of information. Bradner Decl. ¶ 49 (JA.2: 941). These packets are transmitted separately across the Internet circuits described above, and during their journey, they are mixed up with the packets of countless other communications. *Id.* ¶ 104 (JA.2: 959).

Because of how packets are transmitted over the Internet, the NSA cannot know in advance which packets belong to communications to or from its targets. 2d Bradner Decl. ¶¶ 54-58, 68-70, 75-84 (JA.7: 3898-3900, 3903-04, 3906-09). Thus, to identify the communications of its targets on any particular circuit it is monitoring, the NSA must copy all packets of potential interest, reassemble those packets into communications, and review those communications for selectors. *Id.* ¶ 55 (JA.7: 3899).

Indeed, the government's own disclosures make clear that Upstream surveillance involves: (1) the copying of packets on a circuit; (2) the reassembly of

packets into "transactions"; (3) the review of those transactions for the presence of selectors associated with its surveillance targets; and (4) the ingestion of transactions that contain selectors into the NSA's databases. *Id.* ¶¶ 13-16 (JA.7: 3887-88); Bradner Decl. ¶¶ 6(a)-(c), 250-330 (JA.2: 926, 1012-40).[3]

In some instances, the NSA is required to filter the stream of communications to eliminate those packets that are wholly domestic, prior to reassembly and review. Bradner Decl. ¶¶ 290-94 (JA.2: 1025-27). But significantly here, the government's disclosures show that it does not perform any filtering when it conducts Upstream surveillance at "international Internet links." 2d Bradner Decl. ¶¶ 25(e), 35, 42-45 (JA.7: 3890, 3893-95) (discussing the NSA's concession that it "will acquire" wholly domestic communications at the international Internet links it is monitoring).

The NSA seeks "to comprehensively acquire communications that are sent to or from its targets." PCLOB Report 10, 123 (JA.4: 2449, 2562). The "success" of Upstream surveillance depends on the NSA's use of "collection devices that can *reliably* acquire data packets associated with the proper communications." *Id.* at

[3] Until April 2017, the NSA ingested communications that were to, from, or "about" a targeted selector. FISC Mem. Op. & Order 16 (Apr. 26, 2017) (JA.4: 2806). In April 2017, the NSA chose to suspend "about" collection after disclosing that, for years, it had violated court-ordered rules intended to protect Americans' privacy. *Id.* at 19-23 (JA.4: 2809-13).

143, 122-23 (JA.4: 2582, 2561-62) (emphasis added).

D. Surveillance of Wikimedia's Communications

As Wikimedia's expert, Scott Bradner, explains, it is "virtually certain that the NSA has, in the course of the upstream collection program, copied, reassembled and reviewed at least some of Wikimedia's communications." *Id.* ¶ 6(e) (JA.2: 927); 2d Bradner Decl. ¶¶ 3-4 (JA.7: 3883). That conclusion flows from three key facts:

First, Wikimedia's trillions of communications traverse every international Internet link carrying public Internet traffic into and out of the United States. Bradner Decl. ¶¶ 6(d), 336-38, 341-50 (JA.2: 927, 1043-47).

Second, the NSA conducts Upstream surveillance on at least one "international Internet link." [*Redacted*], 2011 WL 10945618, at *15 (FISC Oct. 3, 2011); Bradner Decl. ¶¶ 225, 331-34 (JA.2: 1003, 1040-42).

Third, based on the government's disclosures about the operation, breadth, and goals of Upstream surveillance, the NSA is copying and reviewing some of Wikimedia's communications on each link it is monitoring. 2d Bradner Decl. ¶¶ 17-155 (JA.7: 3888-3938); Bradner Decl. ¶¶ 6-7, 250-370 (JA.2: 926-27, 1012-60).

IV. Procedural History

In 2015, Wikimedia and eight other plaintiffs sued Defendants, claiming that

Upstream surveillance violated the Constitution and FISA. The district court dismissed the suit for lack of standing. This Court vacated the district court's order as to Wikimedia, holding that Wikimedia had plausibly alleged that it was subject to Upstream surveillance. *Wikimedia*, 857 F.3d at 200.

On remand, the district court ordered jurisdictional discovery on Wikimedia's standing.[4] Wikimedia sought both direct and indirect evidence of the surveillance of its communications. Pl. Mot. Compel 3-11 (Mar. 26, 2018), ECF No. 125-2. The government refused to respond to many of Wikimedia's requests, arguing primarily that the information was subject to the state secrets privilege. Wikimedia then moved to compel responses on the ground that FISA's mandatory in camera review procedures displaced the privilege. *See* 50 U.S.C. § 1806(f). The district court denied Wikimedia's motion. *Wikimedia Found. v. NSA*, 335 F. Supp. 3d 772, 790 (D. Md. 2018) (JA.1: 715).

The government then moved for summary judgment. It relied principally on the expert declarations of Henning Schulzrinne, who opined that, as a theoretical matter, it would be possible to design a system of Upstream-"style" surveillance that deliberately ignored Wikimedia's communications. JA.1: 759. The

[4] The district court rejected Wikimedia's argument that the jurisdictional facts were so bound up with the merits as to make bifurcation of the case inappropriate. *See* Order (Sept. 27, 2017), ECF No. 114.

government also argued that further litigation of Wikimedia's standing would reveal state secrets. In response, Wikimedia relied principally on the expert declarations of Scott Bradner. After reviewing the government's extensive public disclosures, Bradner explained it was "virtually certain" that Wikimedia's communications were subject to the NSA's surveillance. JA.7: 3938. Wikimedia also argued that FISA's in camera review procedures displaced the state secrets privilege.

The district court granted the government's motion for summary judgment on December 16, 2019. *Wikimedia Found. v. NSA*, 427 F. Supp. 3d 582, 588 (D. Md. 2019) (JA.7: 4073-74). It held that Wikimedia had not established a genuine dispute of material fact as to its standing, and that further litigation was barred by the state secrets privilege. *Id*.

SUMMARY OF THE ARGUMENT

Wikimedia has presented extensive evidence showing why, based on the government's public disclosures, it is "virtually certain" that some of Wikimedia's trillions of communications are intercepted in the course of Upstream surveillance. Bradner Decl. ¶¶ 6(e), 356 (JA.2: 927, 1049). This evidence is more than enough to establish a genuine dispute of material fact with respect to its standing. The district court erred by failing to credit Wikimedia's evidence as true, by repeatedly drawing inferences against Wikimedia, and by inverting the parties' burdens at

summary judgment—effectively requiring Wikimedia to prove its standing to an absolute "technological" certainty.

Having imposed this heightened burden on Wikimedia, the district court granted summary judgment based on what it conceded was a hypothetical. It credited the government's assertion that, in theory, it would be technically possible for the NSA to filter out all of Wikimedia's communications. JA.7: 4095-96. But neither the district court nor the government identified a single piece of evidence suggesting that the NSA has ever pursued this "Wikimedia-avoidance theory." Moreover, Wikimedia's expert explained at length why this hypothetical is directly contradicted by the government's own disclosures, why it is entirely implausible given the NSA's pursuit of thousands of surveillance targets scattered around the world, and why such an approach would not in fact block access to all of Wikimedia's communications.

Many of the resulting disputes between the parties' experts are highly technical in nature, but fortunately the Court need not resolve them here. Applying the correct standards at summary judgment, Wikimedia has, at a minimum, established a genuine dispute of material fact as to its standing. Based on Wikimedia's evidence, a factfinder could conclude it is more probable than not that some of Wikimedia's communications were being copied and reviewed when its

complaint was filed in 2015.[5] *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992); *Matsushita Elec. Indus. v. Zenith Radio Corp.*, 475 U.S. 574, 587 (1986). Under the Supreme Court's decisions, that is all Wikimedia needs to show at this stage.

Ultimately, the heart of this case is the government's claim that the state secrets privilege bars Wikimedia's surveillance challenge from proceeding, regardless of all the public evidence in the record. For three reasons, this claim is wrong.

First, Congress has foreclosed the government's reliance on the state secrets privilege in surveillance cases like this one. *See Fazaga v. FBI*, 916 F.3d 1202, 1230-34 (9th Cir. 2019). When Congress enacted FISA, it authorized civil suits challenging FISA surveillance and mandated that district courts review sensitive evidence in camera. *See* 50 U.S.C. § 1806(f). FISA's procedures apply here and displace the common-law state secrets privilege. They ensure that the government cannot unilaterally thwart judicial review of sweeping surveillance programs, and they control how this case should proceed. The district court should use FISA's

[5] A plaintiff's standing is evaluated as of the time of the filing of the operative complaint. *See Lujan*, 504 U.S. at 570 n.5. Here, that is 2015, when Wikimedia filed its Amended Complaint. JA.1: 36. Nonetheless, Wikimedia's evidence shows that its injuries are ongoing, and thus the brief at times describes the surveillance in the present tense. The government has not argued that any changes to Upstream surveillance since 2015 defeat Wikimedia's standing today, but if it did, the government would bear the burden of establishing that the case has become moot.

procedures to review in camera any secret evidence bearing on standing or the merits. If the government has any proof that it is *not* in fact intercepting Wikimedia's communications, the court can review that evidence alongside any other purported defenses.

Second, even if FISA's procedures did not apply, the state secrets privilege would not support dismissal—an extraordinary remedy of last resort. Given the government's extensive disclosures about the operation and scope of Upstream surveillance, Wikimedia can establish its standing without resort to privileged evidence, and the government has not shown that the exclusion of any privileged evidence would prevent it from properly defending itself. Because state secrets are not "so central" to Wikimedia's standing that further litigation presents an unacceptable risk of disclosure, dismissal was unwarranted. *El-Masri v. United States*, 479 F.3d 296, 306 (4th Cir. 2007).

Finally, Wikimedia has presented evidence of additional injuries that do not implicate the government's state secrets claim at all. Wikimedia's evidence of lost readership, self-censorship, and mitigation measures provide an alternative basis on which a reasonable factfinder could rely to find standing. And because Wikimedia has standing to sue on its own behalf, it also has standing to sue on behalf of its users.

STANDARD OF REVIEW

This Court reviews de novo the district court's ruling on summary judgment, viewing the facts and all reasonable inferences in the light most favorable to Wikimedia, the non-moving party. *Jacobs v. N.C. Admin. Office of Courts*, 780 F.3d 562, 565 n.1 (4th Cir. 2015).

This Court reviews the district court's exclusion of expert evidence for abuse of discretion. *PBM Prods., LLC v. Mead Johnson & Co.*, 639 F.3d 111, 122-23 (4th Cir. 2011). A court abuses its discretion if it makes an error of law, or if its conclusion rests upon a clearly erroneous factual finding. *Id.*

This Court reviews de novo questions of statutory interpretation, *United States v. Abugala*, 336 F.3d 277, 278 (4th Cir. 2003), including the district court's rulings on the applicability of FISA's in camera review procedures, 50 U.S.C. § 1806(f).

This Court reviews de novo a district court's "legal determinations involving state secrets," including its decision to dismiss a case on state secrets grounds. *El-Masri*, 479 F.3d at 302.

ARGUMENT

I. Wikimedia has presented sufficient evidence of its standing to defeat summary judgment.

To prevail on summary judgment, the government must show that there is no evidence supporting Wikimedia's claim that, when this case was filed, the NSA

was copying or reviewing some of Wikimedia's trillions of communications. Because the record shows, at the very least, a genuine dispute of material fact on this question, the government has not satisfied its burden. In reaching the opposite conclusion, the district court misapplied black-letter law: it inverted the parties' burdens, failed to credit Wikimedia's evidence as true, and repeatedly drew inferences against Wikimedia.

As Wikimedia's expert, Scott Bradner, explains, it is "virtually certain that the NSA has, in the course of the upstream collection program, copied, reassembled and reviewed at least some of Wikimedia's communications." Bradner Decl. ¶ 6(e) (JA.2: 927); 2d Bradner Decl. ¶¶ 3-4 (JA.7: 3883). Bradner's conclusion flows from three key facts. First, as the government concedes, Wikimedia's trillions of communications traverse every circuit on every cable carrying public Internet traffic into and out of the United States. Second, as the government has acknowledged, the NSA monitors communications at one or more of these international Internet links. Third, for reasons Bradner describes at length, the NSA's public descriptions of Upstream surveillance establish that, in 2015 and on an ongoing basis, it has been copying and reviewing some of Wikimedia's communications on each circuit it monitors.

The foundations for Wikimedia's standing showing are at times technically complex, but they are rooted in the government's own disclosures about the

operation, breadth, and goals of Upstream surveillance, understood in light of the technological and practical constraints that the NSA faces in implementing this surveillance. Bradner's opinion is based on these official disclosures and on the expertise he acquired over fifty years of designing, implementing, and operating large-scale networks at Harvard University. His conclusion and the record upon which it is based were more than sufficient to defeat the government's motion.

The government's case for summary judgment, on the other hand, rested on what it admitted was a hypothetical possibility: the claim that, in theory, it would be technically feasible for the NSA to install a set of filters that blocked all of Wikimedia's communications. Rather than provide evidence that Upstream surveillance actually involved the use of such filters, the government enlisted an outside expert, Henning Schulzrinne, to sketch out this hypothetical scenario. Three things are notable about Schulzrinne's submissions. First, he concedes that he has "no knowledge" about whether, in the course of Upstream surveillance, the NSA has ever sought to filter out Wikimedia communications. Schulzrinne Decl. ¶ 53 (JA.2: 743). Second, he does not identify any affirmative evidence supporting his filtering hypothesis; he simply insists it is technically possible. 2d Schulzrinne Decl. ¶ 99 (JA.6: 3450). And third, he conspicuously avoids giving his own expert opinion about what is happening in the real world. That is, he was unwilling even to assert that Upstream surveillance is "likely" avoiding every single one of

Wikimedia's communications.

In accepting this hypothetical exercise as a basis for summary judgment, the court made a fundamental error: it dramatically elevated Wikimedia's burden, requiring Wikimedia to show beyond all doubt that the NSA "must be" copying and reviewing Wikimedia's communications. JA.7: 4109. But no plaintiff is required to prove its case to a perfect certainty—not at summary judgment, and not even at trial, where the standard is a preponderance of the evidence. As the Supreme Court's decisions make clear, to survive summary judgment, Wikimedia must present evidence that a reasonable factfinder could rely on to find standing—*i.e.*, to find it is more probable than not that some of Wikimedia's communications were being copied and reviewed at the time the complaint was filed. Wikimedia's evidence plainly meets that threshold.

A. Legal Standards

Summary judgment may be granted only when there is no genuine dispute of material fact and the movant is entitled to judgment as a matter of law. *See* Fed. R. Civ. P. 56. To prevail, the movant must establish that there is an absence of evidence to support the nonmoving party's case. *Celotex Corp. v. Catrett*, 477 U.S. 317, 325 (1986). In deciding such a motion, a district court may not make credibility determinations but, instead, must accept the nonmoving party's facts as true and draw all reasonable inferences in its favor. *Anderson v. Liberty Lobby,*

Inc., 477 U.S. 242, 255 (1986); *Lujan*, 504 U.S. at 561.

To establish standing, a plaintiff must demonstrate: (1) an injury in fact, (2) a sufficient causal connection between the injury and the conduct complained of, and (3) a likelihood that the injury would be redressed by a favorable decision. *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 157-58 (2014). A plaintiff seeking prospective relief need show only a "substantial risk" of future harm. *See id.* (quoting *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5 (2013)).

In short, to survive summary judgment, a plaintiff "must 'set forth' by affidavit or other evidence 'specific facts'" that would support the elements of standing—evidence that "for purposes of the summary judgment motion *will be taken to be true*." *Lujan*, 504 U.S. at 561 (emphasis added). So long as that evidence shows a genuine dispute of material fact between the parties, summary judgment must be denied.

As explained below, applying these standards properly, Wikimedia has established a genuine dispute of material fact as to its standing.

B. Wikimedia has presented admissible evidence that the NSA is copying and reviewing some of Wikimedia's trillions of communications as they transit international Internet links.

Wikimedia has met its burden at summary judgment by presenting admissible evidence supporting three central facts:

1. Wikimedia's communications traverse every international Internet link carrying public Internet traffic into and out of the

United States.

2. The NSA conducts Upstream surveillance on at least one such Internet link.

3. The NSA is copying and reviewing some of Wikimedia's communications on each link it is monitoring.

Wikimedia relied in part on the expert opinion of Scott Bradner, an Internet networking expert.[6] *See* 2d Bradner Decl. (JA.7: 3880); Bradner Decl. (JA.2: 921). Bradner reviewed dozens of government disclosures describing Upstream surveillance—the NSA's submissions to the FISC, the FISC's opinions, the PCLOB Report, the NSA's targeting and minimization procedures, Defendants' discovery responses, the NSA's deposition testimony, and the NSA's public statements—and he prepared two declarations describing his conclusions and the specific bases for those opinions. Bradner Decl., App'x List (JA.2: 1061). Based on the government's disclosures about Upstream surveillance and based on the volume and distribution of Wikimedia's communications,

[6] Bradner worked at Harvard University from 1966 to 2016 in a variety of technical and educational roles, and he began to develop his expertise in network design when Harvard joined the ARPANET in 1970. He designed and deployed Harvard's earliest data networks, and he was involved in the design of the Longwood Medical Area network and the New England Academic and Research Network. He has served as a consultant on network design, management, and security to educational institutions, federal agencies, international telecommunications enterprises, and commercial organizations. Bradner was also heavily involved in the Internet Engineering Task Force, the primary standards body for Internet technology. Bradner served as Harvard University's Technology Security Officer for eight years. JA.2: 1068.

Bradner concludes that it is "virtually certain that the NSA has, in the course of the upstream collection program, copied, reassembled and reviewed at least some of Wikimedia's communications." *Id.* ¶ 6(e) (JA.2: 927); 2d Bradner Decl. ¶¶ 3-4 (JA.7: 3883).

The district court accepted Wikimedia's evidence as to the first and second prongs of its showing. But it held that Wikimedia's evidence on the third prong did not create a genuine dispute of material fact, notwithstanding Bradner's exhaustively supported opinions. This was error. *See* Part I.C-D, *infra*.

1. It is undisputed that Wikimedia's communications traverse every major Internet circuit entering or leaving the United States.

Due to the volume and distribution of Wikimedia's international communications, those communications travel every possible Internet path into and out of the country. Bradner Decl. ¶¶ 6(d), 336-38, 341-50 (JA.2: 927, 1043-47). The government did not dispute Wikimedia's evidence on this point. JA.7 4091-92. Wikimedia engages in more than a trillion international Internet communications each year, with users in every country on earth. Bradner Decl. ¶¶ 339, 341, 346-47 (JA.2: 1044-46). At the same time, there are about 50 undersea fiber optic cables and relatively few terrestrial cables connecting the U.S. to other countries. *Id.* ¶¶ 201-05, 224 (JA.2: 991-994, 1003).

Undersea fiber cables (Bradner Decl. ¶ 201, JA.2: 992)

Each cable may carry a number of individual circuits, but the circuits connecting the U.S. to the rest of the world are few in number compared to the volume of Wikimedia's communications. *Id.* ¶¶ 200-28, 348 (JA.2: 991-1005, 1046-47). As Bradner observes, "even if there are thousands of international circuits, there would still be hundreds of millions of Wikimedia communications on the average circuit." *Id.*

2. The NSA conducts Upstream surveillance on at least one international Internet link.

The government has acknowledged conducting Upstream surveillance on at least one "international Internet link." Bradner Decl. ¶¶ 291-92 (JA.2: 1025-26) (quoting [*Redacted*], 2011 WL 10945618, at *15). The government declassified and publicly released this fact in a FISC opinion that describes numerous operational details about Upstream surveillance. The NSA admitted at its 30(b)(6)

deposition that the FISC's statement was "accurate," and it adopted the facts contained in the FISC opinion as a whole. JA.1: 445-46, 459-61; *see* Fed. R. Evid. 801(2)(B).

As Bradner explains, an international Internet link or circuit is one that connects a network node outside of the U.S. with a network node inside the U.S. Bradner Decl. ¶ 225 (JA.2: 1003). It is no surprise that the NSA conducts Upstream surveillance on at least one such circuit, because "Internet traffic on international Internet links will consist almost entirely of communications being sent or received (or both) by a node outside the U.S.," *id.*—which are precisely the communications the NSA is permitted to review for selectors under Upstream. *See* PCLOB Report 37-38 & n.140 (JA.4: 2476-77). In concluding that Wikimedia had satisfied this prong of its showing, the district court also relied on a public declaration filed by the Director of National Intelligence. *See* JA.7: 4094; JA.1 184, 186 (acknowledging that the "NSA is monitoring at least one circuit carrying international Internet communications").

Although not necessary to Wikimedia's showing, it bears emphasis that the NSA is monitoring not just a single circuit, but *numerous* circuits as it pursues thousands of targets located around the world. The government itself has publicly acknowledged that, in the course of Upstream surveillance, the NSA monitors multiple circuits. The PCLOB Report repeatedly describes the involvement of

multiple "providers," "circuits," and NSA "collection devices." PCLOB Report 7, 12, 35-40, 85, 143 (JA.4: 2446, 2451, 2474-79, 2524, 2582); *see* JA.5: 3151; [*Redacted*], 2011 WL 10945618, at *10. Moreover, as Bradner explains, given the NSA's many targets, the routing patterns of Internet communications, and the fact that targets move over time, "the NSA is very likely to be monitoring a large number of international circuits." Bradner Decl. ¶ 353 (JA.2: 1048-49); *see id.* ¶¶ 309, 333-34 (JA.2: 1032, 1041-42).[7]

3. Given the government's disclosures about the operation and breadth of Upstream surveillance, it is virtually certain that the NSA is copying and reviewing some of Wikimedia's communications.

Bradner identifies three independent bases for his conclusion that the NSA is copying and reviewing Wikimedia's communications as they traverse international Internet links monitored by the NSA. Yet the district court failed to credit Bradner's technical explanations, failed to draw any inferences in Wikimedia's favor, and improperly resolved the dispute between the parties in the government's

[7] In one of many instances where the district court failed to draw inferences in Wikimedia's favor and engaged in improper factfinding, the court stated that the PCLOB Report's reference to "circuits" did not suggest that the NSA is conducting surveillance on more than one circuit. JA.7: 4093 n.36. But a plain reading of the text is to the contrary. *See* JA.4: 2475 ("The provider is compelled to assist the government in acquiring communications across *these circuits*." (emphasis added)). Moreover, the court did not even engage with the Report's references to multiple "providers" and multiple NSA "collection devices," JA.4: 2446, 2451, 2474-79, 2524, 2582, which would be accurate only if the NSA were monitoring multiple circuits. Bradner Decl. ¶ 353 (JA.2: 1048-49).

favor. *See* Part I.C, *infra*.

First, the technical descriptions in the government's own disclosures show that the NSA is copying and reviewing *all* communications on the international circuits it monitors. As the government conceded to the FISC, the NSA "*will acquire* a wholly domestic 'about' communication if the transaction containing the communication is routed through an international Internet link being monitored by NSA." [*Redacted*], 2011 WL 10945618, at *15 (emphasis added). As Bradner explains, this statement would be true only if the NSA were *not* using any kind of filter at the international links it is monitoring. 2d Bradner Decl. ¶¶ 35-45 (JA.7: 3893-95); *see also id.* ¶¶ 6-8, 25(e) (JA.7: 3884-85, 3890); Bradner Decl. ¶¶ 293-94 (JA.2: 1026-27). And "[t]he lack of all filters on these international Internet links means that the NSA would copy, reassemble and review all communications on the link, *including all Wikimedia communications that happen to be on the link*[.]" 2d Bradner Decl. ¶ 43 (JA.7: 3895) (emphasis added).

The government suggested below that the FISC's description of Upstream was not technically precise, *see* 2d Bradner Decl. ¶ 36 (JA.7: 3893), but there is every reason to believe that the FISC took special care to be so. The opinion describes the court's exacting investigation into a series of government misrepresentations about the technical details of Upstream surveillance, during which the court required the government to submit multiple highly technical

explanations of how the surveillance works. *Id*. ¶¶ 38-39 (JA.7: 3893-94). Moreover, the FISC used equally definitive language to describe the same fact about Upstream surveillance elsewhere in the same opinion. *See* [*Redacted*], 2011 WL 10945618, at *11 ("NSA's upstream collection devices *will acquire* a wholly domestic 'about' SCT if it is routed internationally." (emphasis added)).[8] And finally, the NSA's own witness admitted, in deposition testimony, that this specific statement in the FISC opinion "is accurate." 2d Bradner Decl. ¶¶ 25(c), 40 (JA.7: 3890, 3894) (citing JA.1: 445-46).

Second, Bradner explains that a set of technical and practical necessities make clear that the NSA is copying, reassembling, and reviewing Wikimedia's communications. 2d Bradner Decl. ¶¶ 55-58, 61-112 (JA.7: 3899-3918). As a technical matter, the NSA cannot know in advance whether any given Internet packet crossing a circuit it is monitoring belongs to a transaction containing a selector. *Id.* ¶ 55 (JA.7: 3899). An inherent part of this difficulty is that the NSA is not seeking the communications of a single fixed target, or even a small handful of targets. Instead, the government's public disclosures make clear that Upstream

[8] By contrast, the FISC used a less definitive phrase to describe a slightly different feature of Upstream surveillance just a few paragraphs away. *See* [*Redacted*], 2011 WL 10945618, at *11 n.34 (noting that, given technical limitations in a separate context, the "NSA *may* acquire wholly domestic communications" (emphasis added)).

surveillance is designed to capture the communications of thousands of individuals and groups scattered around the globe. Bradner Decl. ¶ 334 (JA.2: 1042). With so many moving targets, it is impossible for the NSA to know in advance which packets belong to its targets and which do not. *Id.* ¶ 366(d) (JA.2: 1054); 2d Bradner Decl. ¶¶ 54-58, 68-70, 75-84 (JA.7: 3898-3900, 3903-04, 3906-09).

Given this basic technological constraint—and a number of other technical and practical considerations detailed in Bradner's declarations—it is not plausible that the NSA could be making extensive use of filters to actively and specifically avoid Wikimedia's communications. 2d Bradner Decl. ¶¶ 55-58, 61-112, 130-55 (JA.7: 3899-3918, 3926-39). Such filtering is "technologically incompatible with what is publicly known about the upstream collection program." *Id.* ¶ 64 (JA.7: 3902).

Third, the PCLOB has stated, as part of an exhaustive study, that the NSA's goal is to "*comprehensively acquire* communications that are sent to or from its targets." PCLOB Report 10, 123 (JA.4: 2449, 2562) (emphasis added). As both the PCLOB and Bradner emphasize, this goal has certain technological consequences when it comes to surveillance on the Internet. *See* 2d Bradner Decl. ¶¶ 46-50 (JA.7: 3895-97). The reality is that the NSA could not pursue this goal without copying and reviewing all international communications going over the circuits it is monitoring. *Id.* ¶ 54 (JA.7: 3898-99). This is because, as a technological matter, the

NSA could not identify all of the communications of its targets crossing a given circuit *without* reviewing all international communications crossing that circuit for the presence of "selectors." And to review all those communications for selectors, the NSA must first copy and reassemble them. *Id.* ¶¶ 13-16 (JA.7: 3887-88). Since Wikimedia's communications are on every international circuit, "the NSA will be copying, reassembling, and reviewing Wikimedia communications." *Id.* ¶ 54 (JA.7: 3898-99).

Bradner explains each of these three independent bases for his ultimate conclusion—that it is virtually certain that Wikimedia is subject to Upstream surveillance—in meticulous detail. *See id.* ¶¶ 32-112, 130-39 (JA.7: 3892-3918, 3926-30); Bradner Decl. ¶¶ 6-7, 250-81, 290-367 (JA.2: 926-28, 1012-22, 1025-58). Yet the district court refused to credit any of Bradner's technical explanations.

The district court also failed to credit other disclosures corroborating Bradner's analysis. The PCLOB observed, for example, that the type of technology at issue here allows the government "to examine the contents of *all* transmissions passing through collection devices and acquire those, for instance, that contain a tasked selector anywhere within them." PCLOB Report 122 (JA.4: 2561) (emphasis added). The leading treatise on national security investigations, co-authored by the former Assistant Attorney General for National Security, similarly explains that the "NSA's machines scan the contents of *all* of the communications

passing through the collection point, and the presence of the selector or other signature that justifies the collection is not known until *after* the scanning is complete." *See* David Kris & J. Douglas Wilson, Nat'l Security Investigations & Prosecutions 2d § 17.5 (2015) (emphasis in original)). Recent disclosures by the United Kingdom about functionally equivalent surveillance undertaken by the NSA's British counterpart (the GCHQ) state that, "*[f]or technical reasons*, it is necessary to intercept the *entire contents* of a bearer [GCHQ's term for a circuit], in order to extract even a single specific communication for examination from the bearer." Bradner Decl. ¶ 368 (JA.2: 1058) (quoting Further Observations of the Government of the United Kingdom ¶¶ 7-8 (emphases added)); *see also* 2d Bradner Decl. ¶ 146 (JA.7: 3933) (similar UK report). And finally, the U.S. government's EINSTEIN 2 surveillance program, which protects government networks through a similar form of Internet surveillance, likewise involves copying entire streams of traffic, in part to avoid "disrupt[ing] the normal operations of [the systems being monitored]." JA.5: 3161; 2d Bradner Decl. ¶¶ 150-53 (JA.7: 3934-35); Bradner Decl. ¶¶ 283-87 (JA.2: 1023-24).

* * *

For all these reasons, Wikimedia has presented more than sufficient evidence on which a factfinder could rely to find standing—that is, to find it more probable than not that the NSA was copying and reviewing some of Wikimedia's

trillion-plus communications in 2015.

4. The hypothetical scenario advanced by the government's expert cannot support summary judgment in the face of Wikimedia's evidence.

In the district court, the government enlisted an expert, Henning Schulzrinne, to put forward an elaborate hypothetical premised on the claim that, "in theory," it would be technically possible for the NSA to block all of Wikimedia's communications. 2d Schulzrinne Decl. ¶ 99 (JA.6: 3450). In this hypothetical scenario, the NSA would be filtering out, or deliberately ignoring, all traffic to and from Wikimedia's websites. 2d Bradner Decl. ¶ 57 (JA.7: 3900). Neither the government nor Schulzrinne presented a single piece of evidence that the NSA was in fact seeking to block all of Wikimedia's communications. *See* Gov't MSJ Br. 27 (Dec. 7, 2018), ECF No. 164-2. ("None of this is to say that the NSA is, in fact . . . blocking all access to Wikimedia's communications."). Indeed, Schulzrinne concedes that he has "no knowledge" that the NSA is actually taking any of the steps he theorizes. Schulzrinne Decl. ¶ 53 (JA.1: 743). Moreover, as Bradner explains at length, some of Schulzrinne's claims are based on inaccuracies, while others directly conflict with the NSA's public admissions. 2d Bradner Decl. ¶¶ 6-60, 66-96 (JA.7: 3884-3913).

The Court need not wade into each of the disputes between the experts, let alone resolve them. It is doubtful that a purely hypothetical exercise could ever, as

a legal matter, support summary judgment in the face of actual evidence put forward by a plaintiff. *See* Part I.A, *supra*. But regardless, Schulzrinne's declarations present, at most, a dispute of material fact and thus are legally insufficient to support summary judgment.

As Bradner points out, the most obvious flaw with Schulzrinne's filtering theory is that it is directly at odds with the government's own disclosures. 2d Bradner Decl. ¶¶ 7-8, 33-54 (JA.7: 3884-85, 3892-99). Schulzrinne's hypothetical rests on the premise that the NSA could utilize certain types of filtering—"whitelisting" or "blacklisting"—to limit which communications on a circuit it copies and reviews. But this hypothetical filtering is irreconcilable with the FISC's and PCLOB's descriptions of Upstream, discussed above. *See id*. ¶¶ 44, 46-54, 63-112 (JA.7: 3895-99, 3901-18) (discussing the technical implications of the NSA's concession that it "will acquire" certain communications from international internet links it monitors, and the PCLOB's description of the NSA's efforts to acquire its targets' communications "comprehensively"). As the PCLOB Report acknowledges, the NSA has deliberately designed the program to "avoid significant gaps in upstream collection coverage"—yet all of Schulzrinne's theories would create precisely such "blind spots." PCLOB Report 85 (JA.4: 2524); Bradner Decl. ¶¶ 366-67 (JA.2: 1053-58).

Beyond these threshold problems, Bradner painstakingly explains why

Schulzrinne's thought experiment has no traction in the real world, for both technical and practical reasons. 2d Bradner Decl. ¶¶ 6, 55-148, 154-55 (JA.7: 3884, 3899-3939). Below are some, but not all, of the reasons Bradner finds it "entirely implausible" that the NSA would use the approaches Schulzrinne hypothesizes to deliberately ignore all of Wikimedia's communications, Bradner Decl. ¶¶ 366-67 (JA.2: 1053-58):

- Whitelisting IP addresses used by targets: "Whitelisting requires knowing in advance all of the IP addresses that might be used by each of the NSA's targets as well as assuming that those targets are not moving around and thereby changing their IP addresses. This is not remotely possible," particularly because the NSA has thousands of targets. Bradner Decl. ¶ 366(d) (JA.2: 1054); 2d Bradner Decl. ¶¶ 56, 66-89 (JA.7: 3899, 3902-11). This theory is also contradicted by the NSA's "about" collection. *Id.* ¶¶ 108-12 (JA.7: 3917-18).

- Blacklisting all web communications: This theory is directly contradicted by the government's representation that Upstream surveillance involves the collection of "web activity." Bradner Decl. ¶¶ 314-15, 366(f) (JA.2: 1034-35, 1055).

- Blacklisting encrypted communications: This theory ignores that the FISC has granted the NSA permission to retain "all communications that are enciphered," so that it can attempt to decrypt that material. 2d Bradner Decl. ¶¶ 137-39 (JA.7: 3928-30).[9]

- Blacklisting Wikimedia's IP addresses: Bradner describes this theory as "inconceivable" for several reasons. Bradner Decl. ¶ 367(a) (JA.2: 1056). It would needlessly ignore certain communications of the NSA's targets,

[9] Bradner also concludes that, even if the NSA were "blacklisting" HTTPS traffic, "it would still be virtually certain that the NSA would still be copying, reassembling and reviewing Wikimedia HTTP communications considering the number and distribution of those communications." Bradner Decl. ¶ 366(h) (JA.2: 1055).

creating "blind spots," *id.*, without "mak[ing] any measurable difference" in the load on the NSA's system—contrary to Schulzrinne's claim, 2d Bradner Decl. ¶ 96 (JA.7: 3912-13).

Bradner also explains why the kinds of filtering Schulzrinne hypothesizes would not, in fact, be effective at eliminating all Wikimedia communications. Bradner Decl. ¶ 367(b) (JA.2: 1057); 2d Bradner Decl. ¶¶ 57, 97-101 (JA.7: 3900, 3913-15). And finally, Bradner identifies all the conditions that would need to be true in order for the NSA to reliably filter out every single one of Wikimedia's communications. 2d Bradner Decl. ¶¶ 154-55 (JA.7: 3935-39).

In the end, Schulzrinne's Wikimedia-avoidance theory is just that: a theory. Neither the government nor Schulzrinne argues that the theory reflects reality, and they have no adequate response to the many ways in which the theory contradicts what is publicly known about Upstream surveillance. At most, Schulzrinne's declarations present a dispute of material fact—and thus are legally insufficient to support summary judgment.

C. The district court failed to apply the standards governing summary judgment.

1. The district court erred in requiring Wikimedia to establish that the NSA "must be" copying and reviewing its communications.

At nearly every turn, the district court failed to apply the correct legal standards at summary judgment. Most significantly, the court required Wikimedia to establish that the NSA "must be" surveilling Wikimedia's communications as a

matter of "technological necessity"—in essence, to a perfect certainty. This was error.

As the party opposing summary judgment, Wikimedia does not have to establish any fact to an absolute certainty to prevail. It merely has to establish a genuine dispute of material fact. Fed. R. Civ. P. 56. Even at trial, where the standard is a preponderance of the evidence, Wikimedia is not required to establish that the NSA "must be" surveilling its communications. Here, at summary judgment, the issue is simply whether Wikimedia has put forward facts that support the existence of an injury—after taking all Wikimedia's evidence into account, both technical necessity and otherwise. *See* Part I.A, *supra*. And the ultimate question is whether, drawing all inferences in Wikimedia's favor, a factfinder could conclude it is more probable than not that some of Wikimedia's communications were being copied and reviewed in 2015. The answer to that question is undoubtedly yes.

Yet the district court imposed a much higher bar, holding that Wikimedia was required to show that the NSA must be surveilling its communications as a technological necessity. *See, e.g.*, JA.7: 4091. The court seems to have misunderstood Wikimedia's arguments, mistakenly asserting that Wikimedia had "chosen to prove" its standing based solely on this theory. JA.7: 4095 n.41. But Wikimedia has never made such a choice. In addition to presenting evidence that

the NSA must be surveilling its communications as a technological necessity, *see, e.g.*, 2d Bradner Decl. ¶¶ 44-45, 54 (JA.7: 3895, 3898-99), Wikimedia has also presented evidence that for independent technical and practical reasons it is *virtually certain* the NSA is surveilling its communications (even if, in theory, it would be possible to design a system that did otherwise), *see, e.g.*, *id.* ¶¶ 55-60 (JA.7: 3899-3901). The controlling Supreme Court decisions on summary judgment and standing are clear: what Wikimedia must put forward here are "specific facts" that, taken as true, are evidence of injury. *Lujan*, 504 U.S. at 561. Wikimedia has put forward those facts.

2. The district court failed to credit Wikimedia's evidence and improperly resolved disputes between the parties' experts.

Throughout its opinion, the district court repeatedly failed to accept Wikimedia's facts as true and to draw all reasonable inferences in its favor, as required at the summary judgment stage. *See Jacobs*, 780 F.3d at 568-70. Indeed, the court failed to credit *any* of Wikimedia's evidence about the breadth of Upstream surveillance on each circuit—and it ignored Bradner's second declaration altogether. JA.7: 4099-4102.

Three examples illustrate the point. First, the court entirely ignored Bradner's explanation of the government's concession that it "will acquire" wholly domestic "about" communications transiting international Internet links. *See* 2d Bradner Decl. ¶¶ 35-45 (JA.7: 3893-95). As Bradner explains, this means that the

NSA is not using any kind of filter at international Internet links—a fact that directly contradicts Schulzrinne's Wikimedia-avoidance theory. *Id.*[10]

Second, the court failed to credit Bradner's explanation for why the NSA's goal of "comprehensively" acquiring targets' communications requires it to copy and review all international communications transiting the circuits it is monitoring. *See, e.g.*, 2d Bradner Decl. ¶¶ 46-54 (JA.7: 3895-99). Although the court noted that this was one of Bradner's conclusions, JA.7: 4097, it inexplicably pivoted to a discussion of a separate opinion of Bradner's: that the NSA is "most likely" relying on a device with a "copy-then-filter" mechanism to implement Upstream surveillance. *Id.*[11]

Third, the court disregarded Bradner's opinion that blacklisting Wikimedia's IP addresses is implausible in the real world. That opinion is based not only on the government's disclosures, but other technical and practical realities as well: it would not measurably reduce the load on the NSA's systems, would create large holes in a surveillance system intended to be "comprehensive," and would require

[10] The district court suggested that the date of the government's concession might render it irrelevant, in part because Upstream surveillance no longer involves "about" collection. JA.7: 4093-94. But "about" collection did not cease until 2017, and Wikimedia's standing is assessed as of 2015. The government's disclosure from 2011 is plainly probative evidence as to how Upstream surveillance was conducted in 2015. Fed. R. Evid. 401.

[11] The district court devoted much of its factual analysis to this secondary opinion. *See* Part I.D, *infra*.

the NSA to ignore communications that could reveal "what the NSA's foreign intelligence targets are reading and writing." 2d Bradner Decl. ¶ 57, 96 (JA.7: 3900, 3912-13). Instead, the court simply credited Schulzrinne's speculation that Wikimedia's communications could be "low-interest" to the NSA. JA.7: 4100-01. Here, a reasonable factfinder could readily draw the inference that avoiding Wikimedia's communications would have little technical benefit, and would prevent the NSA from reliably collecting the communications of its targets. But rather than drawing all reasonable inferences in Wikimedia's favor, *see Jacobs*, 780 F.3d at 568-70, the court did exactly the opposite.

Running through all these errors was the court's improper resolution of a key dispute between the experts: whether Schulzrinne's filtering theories contradicted the government's own disclosures about Upstream surveillance. *See* 2d Bradner Decl. ¶¶ 7-8, 25, 35-54, 108-12 ("about" surveillance disclosure), 130-36 ("web activity" disclosure), 137-39 (encrypted communications disclosures) (JA.7: 3884-85, 3889-90, 3893-99, 3917-18, 3926-30). Rather than acknowledge the many disputes over the technical meaning of technical documents, the court simply resolved them in one fell swoop—holding that Schulzrinne's hypothetical "does not contradict the government's public disclosures about Upstream surveillance." JA.7: 4101. At summary judgment, this was impermissible.

D. The district court abused its discretion in excluding portions of Wikimedia's expert opinion.

The district court legally erred—and thus abused its discretion—by cursorily excluding paragraphs 282 to 289 of Bradner's first declaration as inadmissible under Federal Rule of Evidence 702 and *Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579 (1993). JA.7: 4097-98. These paragraphs concern Bradner's conclusion regarding the physical configuration that the NSA "most likely" uses to implement Upstream surveillance.

Before explaining why the district court erred, however, it bears emphasis that the excluded paragraphs are independent from the primary bases for Bradner's ultimate conclusion that it is virtually certain that Wikimedia's communications are subject to Upstream surveillance. *See, e.g.*, 2d Bradner Decl. ¶¶ 114-15 (JA.7: 3919-20). The excluded paragraphs instead go to a secondary point: Bradner's view that, at each Internet circuit being monitored, the NSA "most likely" relies on a device that first copies and then filters traffic on the circuit. This secondary point supports Wikimedia's standing, because it shows that the *physical configuration* of Upstream surveillance involves the copying of Wikimedia's communications. *Id.* But even if the Court upheld the district court's exclusion of these paragraphs, that would not call into question Bradner's conclusion that—for entirely independent reasons—Upstream surveillance involves the copying and reviewing of Wikimedia's communications. *See, e.g.*, *id.* ¶¶ 4-60 (JA.7: 3883-3901).

In any event, the district court abused its discretion in excluding these paragraphs. It legally erred by requiring that Bradner have firsthand "knowledge or information" about the NSA's resources, capabilities, and priorities to opine on the likelihood of the copy-then-filter configuration. JA.7: 4097. Under *Daubert*, "an expert is permitted wide latitude to offer opinions, including those that are *not based on firsthand knowledge or observation*." 509 U.S. at 592 (emphasis added). Bradner's opinion also satisfies Federal Rule of Evidence 702, as it is plainly based on "sufficient facts" and his "scientific, technical, [and] other specialized knowledge." Fed. R. Evid. 702(a)-(b). Indeed, it is based on his technical expertise, drawn from decades of experience designing and implementing communications networks at Harvard University; his personal experience working as a consultant to the U.S. government on filtering devices for a similar surveillance program; and the government's own disclosures. *See, e.g.*, Bradner Decl. ¶¶ 9-17, 259, 286, 290-94, 333-35 (JA.2: 928-31, 1014-15, 1024-27, 1041-43); 2d Bradner Decl. ¶ 10 (JA.7: 3886). Ultimately, any doubt about certain facts that Bradner relied upon goes to the weight of the evidence at trial—not to the admissibility of these paragraphs. *See Bresler v. Wilmington Tr. Co.*, 855 F.3d 178, 195 (4th Cir. 2017).

II. The district court erred by refusing to apply the in camera review procedures that Congress mandated in FISA.

Congress enacted FISA to deter unlawful executive branch intelligence activities and to afford meaningful redress to individuals subject to illegal

surveillance. In furtherance of those goals, Congress mandated the use of specific discovery procedures in cases involving foreign intelligence surveillance. 50 U.S.C. § 1806(f). In other contexts where the executive branch asserts that disclosure of materials would harm national security, it may rely on the common-law "state secrets" privilege to exclude certain evidence from a case—and sometimes even to obtain outright dismissal. But Section 1806(f) of FISA reflects Congress's intent to chart a different course in cases challenging government surveillance, by mandating ex parte and in camera judicial review of sensitive information. Through Section 1806(f), Congress struck a careful and deliberate balance to facilitate accountability for unlawful surveillance: it limited the ability of plaintiffs to access sensitive evidence, but at the same time ensured that potentially meritorious claims would be heard and resolved by the courts.

Here, at two different stages of the litigation, the district court misinterpreted this key provision of FISA and refused to apply Section 1806(f) to review in camera evidence that the government claimed was protected by the state secrets privilege.

First, the court wrongly denied Wikimedia's motion to compel discovery and deposition testimony from the government. JA.1: 709, 715. In response to Wikimedia's requests, the government broadly invoked the state secrets privilege to withhold evidence from both Wikimedia and the court. That invocation

triggered Section 1806(f), which displaces the privilege and required the court to review the purportedly sensitive materials in camera. But rather than conduct this review, as FISA commands, the court improperly allowed the government to withhold the evidence as privileged.

Second, the court wrongly dismissed the case on state secrets grounds. JA.7: 4105. FISA's procedures displace the state secrets privilege here and mandate that cases like Wikimedia's be allowed to proceed, with district courts reviewing any sensitive material in camera.

A. The state secrets privilege is no bar to further litigation because Congress displaced the privilege in FISA.

1. In enacting FISA's in camera review provision, Congress intended to regulate discovery of FISA-related information.

In 1976, following a wide-ranging investigation into intelligence abuses, the Church Committee made several recommendations for surveillance reform, including the creation of civil remedies for unlawful surveillance. *See* Church Report, Book II, S. Rep. No. 94-755 at 289, 337 (1976). It envisioned the application of "discovery procedures, including inspections of material in chambers . . . to allow plaintiffs with substantial claims to uncover enough factual material to argue their case." *Id.* at 337.

Largely in response to the Committee's work, Congress enacted civil remedies for unlawful surveillance, together with procedures to ensure effective

judicial review. In Section 1810 of FISA, Congress implemented the Committee's recommendation to authorize individuals to bring civil claims for unlawful surveillance. 50 U.S.C. § 1810. And in Section 1806(f), Congress crafted specific discovery procedures for both criminal and civil cases involving FISA surveillance:

> [W]henever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States . . . to discover or obtain applications or orders or other materials relating to electronic surveillance . . . the United States district court . . . shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted.

50 U.S.C. § 1806(f); *see* H.R. Rep. No. 95-1720, at 31-32 (1978), *reprinted in* 1978 U.S.C.C.A.N. 4048, 4060-61 ("an in camera and ex parte proceeding is appropriate . . . in both criminal and civil cases").[12]

Because Section 1806(f) reflects Congress's decision about how to afford meaningful redress to individuals while accommodating executive branch claims of secrecy, Congress made its procedures mandatory, and it forbade parties from

[12] The House of Representatives originally proposed two separate procedures, one for criminal cases and one for civil cases. *See* H.R. Rep. No. 95-1720, at 31-32. In Section 1806(f), Congress ultimately adopted a single in camera review procedure for courts to apply in both criminal and civil cases.

resorting to other discovery rules concerning FISA-related information. *See* S. Rep. No. 95-604, pt. 1, at 57 (1977).

2. Consistent with Congress's clear intent, Section 1806(f) displaces the state secrets privilege in cases involving FISA surveillance.

A congressional statute abrogates a federal common-law rule, such as the state secrets privilege, if it "'speak[s] directly' to the question addressed by the common law." *United States v. Texas*, 507 U.S. 529, 534 (1993) (citation omitted); *see also* Fed. R. Evid. 501. This displacement doctrine recognizes that Congress's legislative pronouncements supersede the federal courts' common law. *See Milwaukee v. Illinois & Michigan*, 451 U.S. 304, 315 (1981). Through Section 1806(f), Congress spoke directly to the question of how to regulate discovery of FISA-related information—thereby displacing the common-law state secrets privilege.[13] *See Fazaga*, 916 F.3d at 1230-34 (holding that Section 1806(f)'s mandatory procedures displace the state secrets privilege).

The text of Section 1806(f) is deliberately broad in scope and mandatory in application. Its procedures apply whenever "*any* motion or request is made . . . pursuant to *any* . . . statute or rule of the United States" to "discover" materials relating to electronic surveillance. 50 U.S.C. § 1806(f) (emphases added).

[13] *See, e.g.*, *Fazaga*, 916 F.3d at 1227 (observing that "the modern state secrets doctrine" was "[c]reated by federal common law").

These statutory procedures directly map onto, and replace, the common-law rules that govern the executive branch's use of the state secrets privilege in non-FISA cases. The procedures set out in Section 1806(f) "are triggered by a process—the filing of an affidavit under oath by the Attorney General—nearly identical to the process that triggers application of the state secrets privilege, a formal assertion by the head of the relevant department." *Fazaga*, 916 F.3d at 1232. Under Section 1806(f), rather than allow the executive branch to exclude the evidence from the case, the court "shall, notwithstanding any other law, . . . 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). Because Section 1806(f) speaks directly to the circumstances in which the state secrets privilege might otherwise apply, and because it explicitly controls "notwithstanding any other law," it displaces the privilege.

FISA's legislative history confirms Congress's preclusive intent. FISA "put[] to rest the notion that Congress recognizes an inherent Presidential power to conduct such surveillances in the United States outside of the procedures contained in [FISA and Title III]." S. Rep. No. 95-604, pt. 1, at 64; *see also* H.R. Rep. No. 95-1720, at 35 (invoking *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952)). Congress also observed that the common law regulating electronic

surveillance was "uneven and inconclusive. . . . threaten[ing] both civil liberties and the national security." H.R. Rep. No. 95-1283, pt. 1, at 21 (1978). In response, Congress replaced common law that had failed to "adequately balance[] the rights of privacy and national security," *id.*, with provisions, such as Section 1806(f), that "strike[] a fair and just balance between protection of national security and protection of personal liberties," S. Rep. No. 95-604, pt. 1, at 7.

3. The executive branch's reliance on the state secrets privilege to override FISA unconstitutionally infringes on Congress's power.

There is another, fundamental reason that FISA controls in this case and the state secrets privilege does not: the separation of powers between Congress and the executive branch. Because Section 1806(f)'s procedures apply, *see* Part II.B, *infra*, the Constitution forbids the executive branch from relying on the state secrets privilege to shield materials from judicial review. That is because, within the constitutional framework of separated powers, the executive cannot "take[] measures incompatible with the expressed or implied will of Congress," unless the executive's asserted power is both "'exclusive' and 'conclusive' on the issue." *Zivotofsky ex rel. Zivotofsky v. Kerry*, 576 U.S. 1, 10 (2015) (citation omitted).

With respect to the matters addressed by FISA—foreign intelligence surveillance, the handling of sensitive and classified information, and evidentiary rules for U.S. courts—the executive's asserted power is neither "exclusive" nor

"conclusive." *Id.* Congress has the authority to legislate in all three areas, as it has done in FISA and in numerous other statutes. *See, e.g.*, 18 U.S.C. app. 3 §§ 1-16 (Classified Information Procedures Act); 50 U.S.C. §§ 3091, 3125, 3345, 3365 (requiring disclosure of national security information to congressional committees); *see also Vance v. Terrazas*, 444 U.S. 252, 265-66 (1980) (Congress's authority to create evidentiary rules is "undoubted"). Accordingly, separation-of-powers principles forbid the executive branch from thwarting the operation of Section 1806(f) by invoking the state secrets privilege.

B. FISA's in camera review procedures apply here because Wikimedia is an "aggrieved person" under Section 1806(f).

Section 1806(f) applies where an "aggrieved person" seeks to discover or obtain materials related to FISA surveillance. 50 U.S.C. § 1806(f). FISA defines an "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). The district court held, incorrectly, that Wikimedia could not satisfy the "aggrieved person" requirement through plausible allegations—and that it must instead *prove* that it is aggrieved before Section 1806(f)'s procedures apply. JA.1: 708; JA.7: 4113-14. But for the reasons below, Wikimedia's well-pled allegations are more than sufficient to show that it is aggrieved.

The only circuit case on point, *Fazaga v. FBI*, holds that that well-pled

allegations satisfy Section 1806(f)'s "aggrieved person" requirement. 916 F.3d at 1210-11, 1238-39. There, the plaintiffs had alleged that they were subject to unlawful FBI surveillance. *Id.* Although the district court had dismissed several of the plaintiffs' claims on state secrets grounds, the Ninth Circuit reversed, directing the district court on remand to apply Section 1806(f) to review surveillance evidence in camera. *Id.* at 1215, 1251. This holding was based entirely on the allegations in the plaintiffs' complaint. *Id.*; *see also In re NSA Telecomm. Records Litig.*, 595 F. Supp. 2d 1077, 1083 (N.D. Cal. 2009) (rejecting argument that "only affirmative confirmation by the government or equally probative evidence will meet the 'aggrieved person' test").[14]

The "plausible allegations" standard comports with the text and structure of the statute, as well as common sense. FISA was designed to permit civil claims to proceed by channeling discovery through Congress's chosen procedures. *See* Part II.A.1-2, *supra*. In civil litigation, discovery necessarily occurs before plaintiffs are required to prove their case. It would be entirely illogical to require FISA plaintiffs

[14] One district court in California initially applied Section 1806(f)'s procedures on the basis of the plaintiffs' allegations, *see* Order 12-15, *Jewel v. NSA*, No. 08-cv-04373 (N.D. Cal. July 23, 2013), ECF No. 153, but following its in camera review, improperly resurrected the state secrets privilege as a basis for granting summary judgment to the government, *see* Order 18-25, *Jewel*, No. 08-cv-04373 (N.D. Cal. Apr. 5, 2019), ECF No. 462. The plaintiffs' appeal in that case is pending.

to *prove* that they have been subject to electronic surveillance—potentially requiring a trial on standing—before Section 1806(f)'s discovery procedures applied. Indeed, such a rule would require courts to bifurcate every civil case challenging FISA surveillance, except where the government admitted that the plaintiff was aggrieved. In the first phase, FISA plaintiffs would be required to prove they were aggrieved *and* would have to overcome the government's assertion of the state secrets privilege on that very question. Only after those extensive proceedings, during a second phase, could district courts actually apply the procedures that FISA mandates. Unsurprisingly, the statute contains no such requirement—and does not even hint at such a complex scheme. The correct interpretation of Section 1806(f) is the one that appears on the face of the statute, *Conn. Nat'l Bank v. Germain*, 503 U.S. 249, 253-54 (1992), and corresponds to the ordinary sequence of civil litigation: pleadings; then discovery, using FISA's procedures; then proof.

This interpretation also comports with Congress's overriding purpose in enacting FISA, which was to ensure judicial review of executive branch surveillance. If a plaintiff had to prove it was aggrieved before FISA's procedures attached—and the government remained free to assert the state secrets privilege in the interim, just as it's done here—the executive branch would retain nearly exclusive control over challenges to FISA surveillance. *See Fazaga*, 916 F.3d at

1237 (permitting a FISA claim "to be dismissed on the basis of the state secrets privilege because the § 1806(f) procedures are unavailable . . . would undermine the overarching goal of FISA more broadly"). An interpretation of Section 1806 that handed the executive branch such power would be entirely at odds with Congress's intent. It would profoundly undermine the civil remedies that Congress enacted for surveillance abuses, and the very purpose of FISA itself. *See* 50 U.S.C. § 1810; 18 U.S.C. § 2712.[15]

Yet the district court's interpretation of FISA gave the government precisely that power to thwart surveillance challenges. The court concluded, incorrectly, that Wikimedia had to *prove* that it was aggrieved for Section 1806(f) to apply. JA.1: 708; JA.7: 4113-14. Wikimedia highlights several of the court's errors below.

First, the court mistakenly applied the canon of ejusdem generis—*i.e.*, construing general words in a list with reference to earlier, more specific items—in interpreting Section 1806(f). JA.1: 700-02. That canon of construction is entirely inapposite here. Like all interpretive canons, it applies only where statutory language is ambiguous, *see Garcia v. United States*, 469 U.S. 70, 73-75 (1984), but there is no ambiguity about the text of Section 1806(f). The statute applies in three

[15] Of course, even if the Court were to conclude that Wikimedia must adduce evidence sufficient to survive summary judgment before Section 1806(f)'s procedures apply, Wikimedia is one of the rare plaintiffs capable of adducing such evidence—and has done so. *See* Part I, *supra*.

scenarios: (1) when the government provides notice to a defendant; (2) when a defendant moves to suppress FISA-related evidence; and (3) when any motion to discover FISA-related material is made by an aggrieved person. 50 U.S.C. § 1806(f). The court believed that, in the first two scenarios, "there is clear evidence that electronic surveillance has occurred," and it misapplied ejusdem generis to conclude that the third scenario requires an evidentiary showing as well. JA.1: 701. This was a gross distortion of the canon, which is designed to ascribe meaning to a "general or collective term following a list of specific items"—for example, "hooks, bobbers, sinkers, *and other equipment*." *CSX Transp., Inc. v. Ala. Dep't of Revenue,* 562 U.S. 277, 294-95 (2011) (emphasis added). Of course, Section 1806(f) features no such list. This Court could only conceivably apply ejusdem generis if there were uncertainty about the meaning of "any other statute or rule" in Section 1806(f). There is not. Congress simply mandated that litigants could not rely on statutes or rules *other than FISA* to discover this particular type of evidence.

In misapplying this canon, the district court also ignored clear differences among the three scenarios that the statute addresses. While the first two scenarios address prosecutions and other proceedings where the government is *affirmatively* seeking to use evidence obtained from FISA, the third scenario is deliberately broader: it covers any case, including civil suits, where a person seeks to discover

FISA-related evidence showing they were unlawfully surveilled.[16] Congress recognized that these cases would involve discovery—which logically precedes a plaintiff's evidentiary showing—and it required plaintiffs to use FISA's specialized procedures. *See* H.R. Rep. No. 95-1720, at 31-32.

Second, the district court misinterpreted Section 1806(f)'s requirement that courts review FISA material in camera to assess whether surveillance was "lawfully authorized or conducted." The court reasoned that because "it is impossible to determine the lawfulness of surveillance if no surveillance has actually occurred," Section 1806(f)'s procedures required Wikimedia to first prove that it was aggrieved. JA.1: 699. But once a plaintiff has survived a motion to dismiss, in camera review to resolve standing is entirely consistent with the language of Section 1806(f). The district court's analysis of standing is simply the first step in "determin[ing] whether the surveillance of [Wikimedia] was lawfully authorized and conducted." 50 U.S.C. § 1806(f). Moreover, the standing and merits questions here are intertwined: the question of whether Wikimedia's communications have been subjected to Upstream surveillance goes to both.

[16] The court was also incorrect that the second scenario—a motion to suppress pursuant to 50 U.S.C. § 1806(e)—requires "clear evidence" of surveillance. Defendants may seek to suppress evidence regardless of whether the government has given notice of surveillance pursuant to Section 1806(c) or (d). *United States v. Belfield*, 692 F.2d 141, 146 (D.C. Cir. 1982).

Third, the district court concluded, wrongly, that even if government notice of surveillance were a prerequisite to the application of Section 1806(f), that would be consistent with Congress's overall scheme. JA.1: 705. Not so. The district court's approach would give the government complete control over civil challenges to FISA surveillance, contrary to Congress's intent. *See* H.R. Rep. No. 95-1720, at 31-32. Addressing FISA's civil remedy, the court reasoned that because only individual-capacity claims are available under Section 1810, the government would presumably cooperate with Section 1810 plaintiffs by providing notice. JA.1: 705-06. But those suits would predictably involve information that the government considers to be classified—giving the government every reason to withhold notice from Section 1810 plaintiffs, or to intervene in the suit to assert the state secrets privilege.[17]

Finally, the district court misinterpreted the only circuit law on point, *Fazaga v. FBI*. JA.7: 4113-14 & n.60. It concluded that *Fazaga* "says nothing" about the application of Section 1806(f) here, focusing on a single sentence of the *Fazaga* court's opinion: "[t]he complaint's allegations are sufficient if proven to establish that Plaintiffs are 'aggrieved persons.'" JA.7: 4113 (quoting 916 F.3d at

[17] The district court simply ignored the fact that the United States is subject to actions under 18 U.S.C. § 2712, and that remedy also relies on FISA's in camera review procedure.

1216). But in this sentence, the *Fazaga* court was addressing an entirely different question, as the surrounding discussion and section header make plain: whether the plaintiffs had stated a claim under *Section 1810*—not whether Section 1806(f) applied. With respect to Section 1806(f), the Ninth Circuit in *Fazaga* was clear: it ordered the district court to apply the statute's in camera procedures on remand, based on the plaintiffs' well-pled allegations that they were aggrieved. 916 F.3d at 1251. *Fazaga* squarely supports Wikimedia's argument.[18]

III. Even if FISA's in camera review procedures do not apply, the district court erred in dismissing the case on state secrets grounds.

Even if the state secrets privilege were available in this case, it would not warrant dismissal, as Wikimedia can establish its standing based on information the government has already made public.

A. Courts carefully scrutinize invocations of the state secrets privilege, especially when dismissal is sought.

Where the state secrets privilege properly applies, it allows the government to withhold evidence due to a "reasonable danger" that disclosure will "expose military matters which, in the interest of national security, should not be divulged."

[18] Among the district court's other errors, it observed that "statutes in derogation of the common law should be narrowly construed," cherry-picking language from a Supreme Court dissent (without acknowledging that the language came from a dissenting opinion). JA.1: 702. This standard is inconsistent with the larger body of cases addressing common law displacement. *See Texas*, 507 U.S. at 534 (to abrogate common law, statute must "speak directly" to the issue).

United States v. Reynolds, 345 U.S. 1, 10 (1953). Courts closely scrutinize the government's claims of this privilege, also known as the *Reynolds* evidentiary privilege, to "ensure that [it] is asserted no more . . . sweepingly than necessary." *Abilt v. CIA*, 848 F.3d 305, 312 & n.5 (4th Cir. 2017) (quotation marks omitted). "Appropriate judicial oversight is vital to protect against the 'intolerable abuses' that would follow an 'abandonment of judicial control'" over the application of the privilege. *Id.* (quoting *Reynolds*, 345 U.S. at 8).

Even where a court has determined that an invocation of the *Reynolds* privilege is valid, the result is simply that "[t]he privileged information is excluded and the trial goes on without it." *Gen. Dynamics Corp. v. United States*, 563 U.S. 478, 485 (2011). In contrast, in a narrow category of disputes over sensitive government contracts—so-called *Totten*-bar cases—state secrets completely bar judicial review. *See Totten v. United States*, 92 U.S. 105, 107 (1875); *Reynolds*, 345 U.S. at 11.

In cases like this one, involving the *Reynolds* privilege, the Fourth Circuit requires dismissal only if: (1) the plaintiff cannot establish its prima facie case without the privileged evidence; (2) the defendant cannot "properly" defend itself without the evidence; or (3) state secrets are "so central" to the litigation that "any attempt to proceed" would present an "unjustifiable risk of disclosure." *Abilt*, 848 F.3d at 313-14 (citations omitted). The first scenario is a straightforward

application of the *Reynolds* rule: the evidence is excluded, and the case continues (insofar as it can). The second and third scenarios are exceptions to that rule and must be construed narrowly, to avoid conflating the *Reynolds* evidentiary privilege with the *Totten* justiciability bar.[19] A court must carefully scrutinize the government's assertions and determine for itself whether litigation may go forward, in light of the judiciary's constitutional "duty . . . to say what the law is." *Marbury v. Madison*, 5 U.S. (1 Cranch) 137, 177 (1803). Courts therefore use "creativity and care" to devise "procedures which will protect the privilege and yet allow the merits of the controversy to be decided in some form." *Fitzgerald v. Penthouse Int'l, Ltd.*, 776 F.2d 1236, 1238 n.3, 1241 n.7 (4th Cir. 1985). Dismissal is available only as a last resort.

B. The privilege does not support dismissal of the case.

The district court erred in holding that the state secrets privilege prevents further litigation of Wikimedia's standing.

Wikimedia need not rely on privileged evidence to establish its prima facie case for standing, *i.e.*, that as of 2015, some of its communications were being copied and reviewed. *See* Part I.B, *supra*. Accordingly, this case is not like others the Court has dismissed on state secrets grounds, in which plaintiffs could not

[19] While *Abilt* is the law of the Circuit, its third scenario wrongly collapses the *Reynolds* privilege and the *Totten* bar. *See Gen. Dynamics*, 563 U.S. at 485.

establish key elements of their claims without relying on privileged evidence. *See, e.g.*, *El-Masri*, 479 F.3d at 309. Here, the public record alone is enough.

Moreover, the exclusion of privileged evidence from this case will not make it impossible for the government to "properly defend" itself. JA.7: 4110. In the proceedings below, the government never asserted that the exclusion of privileged evidence would in fact deprive it of a legitimate defense. It merely raised the possibility of a *hypothetical* defense—one based on Schulzrinne's thought experiment, in which the NSA could "in theory" avoid copying or reviewing any one of Wikimedia's trillions of communications. *See* Part I.B.4, *supra*. Before accepting the government's argument that it could not properly defend itself, the district court never reviewed the purportedly privileged material in camera, and never even considered the validity of the government's hypothetical defense. For at least three reasons, this was error.

First, "[a]llowing the mere prospect of a privilege defense, without more, to thwart a citizen's efforts to vindicate his or her constitutional rights would run afoul" of Supreme Court precedent, which cautions against "broadly interpreting evidentiary privileges" and "precluding review of constitutional claims." *Fazaga*, 916 F.3d at 1253 (citing, *inter alia*, *United States v. Nixon*, 418 U.S. 683, 710 (1974) (evidentiary privileges should not be "expansively construed, for they are in derogation of the search for truth")).

Second, both the D.C. and Ninth Circuits have held that, to obtain dismissal on the ground that the *Reynolds* privilege precludes a defense, the government must establish to the court that the privilege actually precludes a legally *meritorious* defense—one that would require judgment for the defendant. *In re Sealed Case*, 494 F.3d 139, 149-50 (D.C. Cir. 2007); *Fazaga*, 916 F.3d at 1253. As these courts have persuasively explained, "[w]ere the valid-defense exception expanded to mandate dismissal of a complaint for any plausible or colorable defense, then virtually every case in which the United States successfully invokes the state secrets privilege would need to be dismissed." *In re Sealed Case*, 494 F.3d at 149-150. To assess the validity of a privileged defense, a reviewing court must conduct an "appropriately tailored *in camera* review of the privileged record." *Id.* at 151. Although the Fourth Circuit has not squarely considered whether the "valid defense" doctrine applies, it has cited approvingly to the case establishing (and narrowly defining) the doctrine. *See Fitzgerald*, 776 F.2d at 1241 n.7, 1242 (citing *Molerio v. FBI*, 749 F.2d 815, 822-26 (D.C. Cir. 1984)). This Court has also "instructed the district court to consider [state secrets-]privileged evidence *in camera*" to assess the validity of an immunity defense. *Id.* at 1243 n.12 (discussing *Heine v. Raus*, 399 F.2d 785, 791 (4th Cir. 1968)).

Unlike the district court's approach, the reasoning of the D.C. and Ninth Circuits adheres to *Reynolds*'s "formula of compromise," and its command that

"[j]udicial control over the evidence in a case cannot be abdicated to the caprice of executive officers." 345 U.S. at 9-10. While in camera review of privileged material is not "automatically require[d]" in every case in which the government seeks merely to withhold evidence, *id.* at 10, such review must at least be required where, as here, the government seeks to dismiss an entire suit on the theory that it cannot present a valid defense. *See Fazaga*, 916 F.3d at 1253.

Third, even if this Court does not require the government to establish the *validity* of its defense, at a minimum, the government must be required to establish the *existence* of its privileged defense in camera. It is axiomatic that the government cannot invoke the state secrets privilege over non-existent evidence. Here, the district court should be required to assess whether there is, in fact, a defense to which the privilege might attach. *See El-Masri*, 479 F.3d at 305 ("a court may conduct an in camera examination of the actual information sought to be protected"). If the government does not possess evidence that Upstream surveillance involves complete avoidance of all of Wikimedia's communications, as Schulzrinne hypothesizes, then there is simply no information to which the *Reynolds* privilege could apply.

Finally, the district court was simply incorrect that the "whole object" of adjudicating Wikimedia's standing is to "establish a fact that is a state secret." JA.7: 4110-11 (citation omitted). To find that Wikimedia has standing, the district

court need not conclusively determine that Wikimedia is or was in fact subject to Upstream surveillance. Rather, it need only find that, as of 2015, some of Wikimedia's trillions of communications were at *substantial risk* of being copied and reviewed. *See* Part I.A, *supra*. The existence of such a risk is not itself a state secret, nor would a judicial ruling based on the public record reveal anything the public does not already know. That is especially true here because the record is clear that (1) the government monitors *at least* one international circuit in the United States, and (2) Wikimedia sends voluminous Internet traffic over *every* international circuit in the United States. *See* JA.7: 4095. Moreover, the NSA has already acknowledged that it is monitoring "web activity"—precisely the type of web communications that Wikimedia engages in more than a trillion times each year. Bradner Decl. ¶¶ 314-15, 344 (JA.2: 1034-35, 1045); *see also* JA.5: 2920. Accordingly, state secrets are not "so central" to Wikimedia's standing that further litigation presents an unacceptable risk of disclosure. *Abilt*, 848 F.3d at 314.[20]

[20] The district court likewise erred in upholding the government's assertion of the privilege over seven broad categories of information. JA.1: 712-13. Given the government's extensive public disclosures, not all information within those categories is privileged. For example, the court upheld the privilege as to "categories of Internet-based communications subject to Upstream"—such as whether the surveillance involves the collection of HTTP and HTTPS communications. JA.1: 712, 715 n.18. But the government has already disclosed its Upstream collection of "web" communications, which are by definition HTTP and HTTPS communications. Bradner ¶¶ 7(b), 314-15 (JA.2: 927-28, 1034-35).

IV. Wikimedia has suffered additional injuries that independently establish its standing.

Wikimedia has presented evidence of additional injuries that independently establish its standing.

Specifically, as Wikimedia's expert Dr. Jonathon Penney explained, Upstream surveillance has impaired Wikimedia's communications with its community members by, among other things, causing a steep and statistically significant drop in the readership of certain Wikimedia pages. JA.3: 2163-64; JA.3: 2235-37; JA.3: 2246-52.

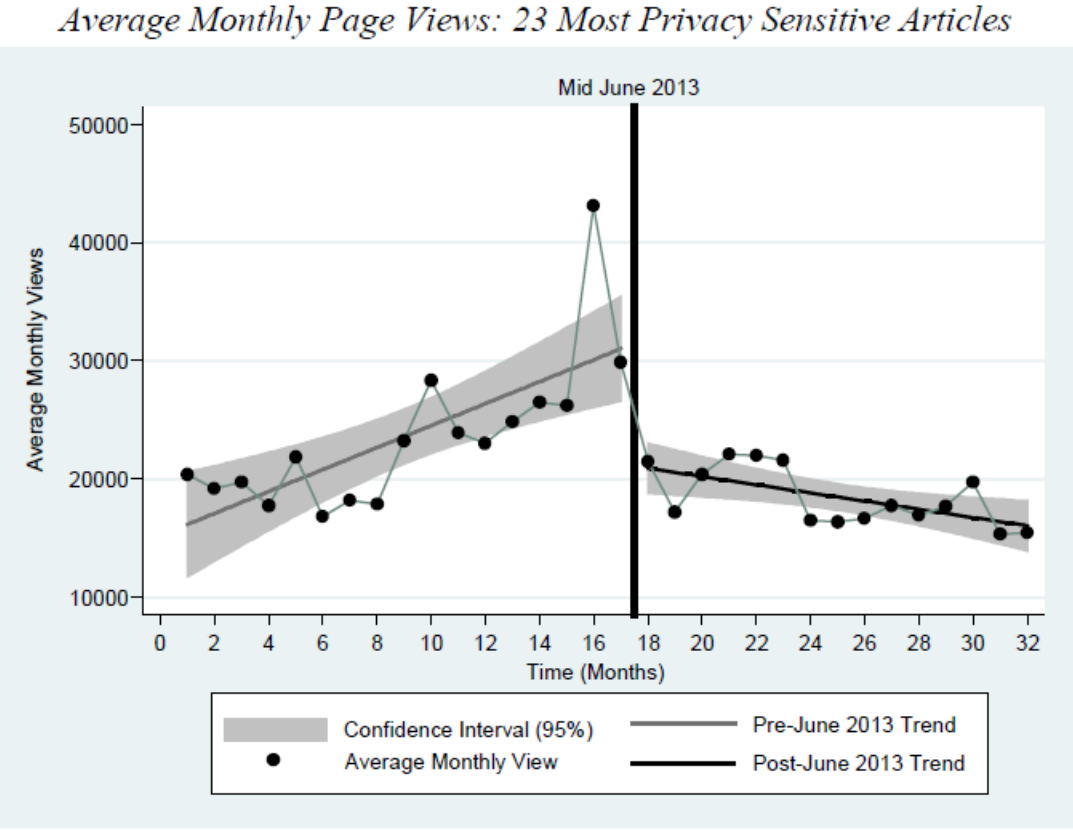

Chart showing decline in readership of certain Wikipedia pages 2d Penney Decl. ¶ 15 (JA.7: 3956)

And Wikimedia has taken reasonable but costly measures to mitigate the risk of Upstream surveillance of its communications. *See* JA.3: 2237-2242 (explaining implementation of costly new protocols to encrypt Wikimedia's communications, requiring several years' worth of employee work and an expenditure of more than $300,000). These injuries were driven by the revelations beginning in 2013 about the existence, breadth, and operation of Upstream surveillance, including the publication by the press of multiple NSA slides showing that the NSA was surveilling Wikimedia's communications. JA.5: 3221, 3246.

NSA slide published in *The Guardian* (JA.5: 3221)

These harms constitute concrete injuries-in-fact that are directly traceable to Upstream surveillance. *See Wikimedia*, 857 F.3d at 211. Yet the district court

attributed all of these injuries to "subjective and speculative fears of government surveillance," inadequate to establish standing under *Clapper*, 568 U.S. 398. JA.7: 4115 n.62. But that case was nothing like this one. Here, Wikimedia's theory of standing does not rely "on a highly attenuated chain of possibilities." *Clapper*, 568 U.S. at 410, 416. Rather, it relies on a single and straightforward conclusion: that a surveillance program designed to systematically scan streams of Internet communications on international circuits poses a substantial risk of scanning some of Wikimedia's ubiquitous Internet communications on those circuits.

As the Supreme Court has recognized, costly protective measures confer standing when they are undertaken to prevent or mitigate known, significantly likely harms. *See Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 153 n.3, 155 (2010) ("Such harms, which respondents will suffer even if their crops are not actually infected with the Roundup Ready gene, are sufficiently concrete[.]"). Here, Wikimedia's evidence that some of its many communications will be intercepted as they travel across circuits monitored by the NSA is, if anything, even stronger than the alfalfa farmers' predictions about the movements of the bees in *Monsanto*. *Id*.[21]

[21] Contrary to the district court's claim, the fact that Upstream surveillance was not the sole reason Wikimedia adopted some of its mitigation measures is no bar to redressability. JA.7: 4117 n.63; *see Monsanto*, 561 U.S. at 155; *Larson v. Valente*, 456 U.S. 228, 243 n.15 (1982).

V. If Wikimedia has standing, it also has third-party standing to assert the rights of its community members.

Finally, the district court erred in hastily rejecting Wikimedia's showing that it has third-party standing to assert the rights of certain users.[22] This issue is critical because Wikimedia's users have their own privacy and expressive interests in the communications the government is intercepting, and they face obvious obstacles to litigating their own rights. As the record makes plain, Wikimedia has presented evidence that satisfies the conditions for third-party standing. *See Kowalski v. Tesmer*, 543 U.S. 125, 129-30 (2004).

First, Wikimedia presented evidence of its own injuries-in-fact, for all the reasons set out above. Second, Wikimedia presented evidence establishing its close relationship with its users, which depends heavily on the privacy and confidentiality of those users' communications with Wikimedia. JA.3: 2221-23; JA.7: 4007-11; JA.3: 2271-72. Given this relationship, Wikimedia will be an effective proponent of its users' rights. Third, because Wikimedia's users could not file suit without sacrificing the very online privacy and anonymity that this lawsuit

[22] Those users are: (1) individual users inside the U.S. whose communications with Wikimedia servers abroad are subject to Upstream surveillance; (2) U.S. persons abroad whose communications with Wikimedia servers in the U.S. are subject to Upstream surveillance; and (3) individual users inside the U.S. whose ability to exchange information with Wikimedia's foreign readers and editors has been impaired by Upstream surveillance. Bradner Decl. ¶¶ 353-54 (JA.2: 1048-49); JA.4: 2397; JA.3: 2249; JA.7: 4013-14; JA.7: 4016-18.

seeks to protect, they face clear obstacles to litigating their own rights. JA.3: 2274-77; JA.7: 4016-18. Once again, the district court simply rejected Wikimedia's evidence—the opposite of what it was required to do at summary judgment. JA.7: 4117. And contrary to the court's conclusion, the relationship between Wikimedia and its users plainly satisfies the second *Kowalski* factor. *See Connection Distrib. Co. v. Reno*, 154 F.3d 281, 295 (6th Cir. 1998); *Enterline v. Pocono Med. Ctr.*, 751 F. Supp. 2d 782, 786 (M.D. Pa. 2008). Similarly, the district court failed to credit Wikimedia's factual showing about the obstacles that individual users would face in seeking to vindicate their own privacy and expressive rights, dismissing that evidence out of hand. JA.7: 4118 n.67. At summary judgment, that was improper.

CONCLUSION

For the foregoing reasons, the Court should reverse the district court's orders granting the government's motion for summary judgment and denying Wikimedia's motion to compel. The Court should remand the case with instructions for the district court to apply Section 1806(f)'s procedures to review any sensitive FISA information relevant to standing or the merits in camera, using appropriate security procedures.

July 1, 2020

Respectfully submitted,

/s/ *Patrick Toomey*

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

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

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

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

REQUEST FOR ORAL ARGUMENT

Due to the novel and significant legal issues in this case, Plaintiff–Appellant respectfully requests oral argument pursuant to Local Rule 34(a).

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because it contains 14,996 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: July 1, 2020

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