IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION,

Plaintiff,

v.

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

Defendants.

Hon. T. S. Ellis, III

Civil Action No. 15-cv-00662-TSE

PLAINTIFF WIKIMEDIA FOUNDATION'S BRIEF IN OPPOSITION TO DEFENDANTS' MOTION FOR SUMMARY JUDGMENT

David R. Rocah (Bar No. 27315)
Deborah A. Jeon (Bar No. 06905)
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 (pro hac vice)
Ashley Gorski (pro hac vice)
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

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

Alex Abdo (pro hac vice)
Jameel Jaffer (pro hac vice)
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

Table of Contents

Table of Authorities ii

Introduction 1

Background and Prior Proceedings 2

Statement of Facts 3

I. Wikimedia's statement of undisputed material facts 3

II. Response to Defendants' statement of undisputed material facts 9

Argument 11

I. Wikimedia has standing. 11

A. Legal standards 13

B. As Wikimedia's expert explains, it is a virtual certainty that the NSA is copying and reviewing some of Wikimedia's trillions of Internet communications. 13

1. Based on the government's official disclosures, it is virtually certain that the NSA is copying and reviewing at least some of Wikimedia's trillions of Internet communications. 15

2. The government's expert declaration is flawed and does not address the question of whether the NSA is copying and reviewing Wikimedia's communications. 20

C. Wikimedia has suffered additional injuries that establish its standing. 25

1. Upstream surveillance has impaired Wikimedia's activities and ability to communicate with its community members. 25

2. Upstream surveillance has required Wikimedia to take costly protective measures. 27

D. Wikimedia has third-party standing to assert the rights of its users. 27

II. The government's state secrets arguments are meritless. 28

Conclusion 30

Table of Authorities

Cases

Abilt v. CIA,
848 F.3d 305 (4th Cir. 2017) 29, 30

Anderson v. Liberty Lobby, Inc.,
477 U.S. 242 (1986) 13

Celotex Corp. v. Catrett,
477 U.S. 317 (1986) 13

Clapper v. Amnesty Int'l USA,
568 U.S. 3985 (2013) 13, 26, 27

Kowalski v. Tesmer,
543 U.S. 125 (2004) 28

Laird v. Tatum,
408 U.S. 1 (1972) 26

Lujan v. Defs. of Wildlife,
504 U.S. 555 (1992) 13

Monsanto Co. v. Geertson Seed Farms,
561 U.S. 139 (2010) 27

Sterling v. Tenet,
416 F.3d 338 (4th Cir. 2005) 30

Susan B. Anthony List v. Driehaus,
573 U.S. 149 (2014) 13

United States v. Ancient Coin Collectors Guild,
899 F.3d 295 (4th Cir. 2018) 21

United States v. Reynolds,
345 U.S. 1 (1953) 29

Wikimedia Found. v. NSA,
2018 WL 3973016 (D. Md. Aug. 20, 2018) 28, 30

Wikimedia Found. v. NSA,
857 F.3d 193 (4th Cir. 2017) 3, 26

Statutes

50 U.S.C. § 1806 30

50 U.S.C. § 1881a 19

Rules

Fed. R. Civ. P. 56 13

Fed. R. Evid. 702 21

Other Authorities

H.R. Rep. No. 95-1720 (1978), *reprinted in* 1978 U.S.C.C.A.N. 4048 30

Introduction

Wikimedia clearly has standing. As Wikimedia's expert explains, it is a "virtual certainty" that the NSA is copying and reviewing at least some of Wikimedia's trillions of Internet communications in the course of Upstream surveillance. Wikimedia's communications are so numerous, so widely distributed, and so intermingled with other international Internet communications that some of them are undoubtedly subject to NSA monitoring. Given the government's public disclosures about Upstream surveillance, the technological necessities of surveillance on the Internet, and the NSA's stated objectives, this is not a close question.

By contrast, the government seeks summary judgment based on a series of hypothetical possibilities. Its expert ignores key features of Upstream surveillance the government has disclosed. And remarkably, he never opines on the most important issue before the Court: the likelihood that the NSA is intercepting some of Wikimedia's trillions of communications. Instead, the government's expert concedes that he has no knowledge of whether the NSA actually employs any of the approaches he offers. And he takes no position on whether the NSA is, in fact, using any of those approaches—let alone in a way that would avoid *every single one* of Wikimedia's trillions of communications. As Wikimedia's expert, Scott Bradner, explains, some of the government's hypotheticals are based on technical inaccuracies, while others directly conflict with the NSA's public admissions.

Ultimately, the government turns the summary judgment standard on its head. The government suggests that, in order to prevail, Wikimedia must disprove each of its expert's theoretical possibilities to show that the NSA "must be" copying and reviewing Wikimedia's communications. But that is not Wikimedia's burden—not even at trial. At this stage of the case, Wikimedia need only show a genuine dispute of material fact concerning the copying or review of its communications—and there is no question that it has done so.

Wikimedia has also provided evidence of injuries beyond the interception of its communications. As a statistical study by Dr. Jonathon Penney shows, NSA surveillance, including Upstream surveillance, is "highly likely" to have caused the significant and lasting drop in readership of certain Wikipedia pages that followed the June 2013 revelations about the scope of the NSA's surveillance. In response to this surveillance, Wikimedia has taken costly protective measures to better secure its communications and mitigate the harms to its mission. These injuries, too, support Wikimedia's standing.

Finally, Defendants argue that the state secrets privilege precludes the Court from ruling on the basis of the government's extensive *public* admissions about Upstream surveillance. That argument is wrong, and it is flatly contradicted by the Court's prior opinion, which held that Wikimedia is entitled to make its showing at summary judgment on the public record. Defendants seek to relitigate an extraordinary claim that Congress and the Court have rejected: that the Executive Branch alone controls who can and cannot challenge unlawful surveillance.

Background and Prior Proceedings

This lawsuit challenges the suspicionless seizure and searching of Internet traffic by the National Security Agency on U.S. soil. According to the government's own disclosures, the NSA is systematically searching through international Internet communications for those associated with thousands of foreign individuals and groups. This surveillance dragnet, called Upstream surveillance, involves an unprecedented invasion of the privacy of countless Americans. Using NSA-designed surveillance devices, the government monitors Internet traffic entering and leaving the U.S., reviewing vast quantities of emails and web activity in deciding which communications to keep. Wikimedia's communications are caught in this surveillance dragnet.

In prior proceedings, the Fourth Circuit held that Wikimedia had plausibly alleged standing: "To put it simply, Wikimedia has plausibly alleged that its communications travel all

of the roads that a communication can take, and that the NSA seizes all of the communications along at least one of those roads." *Wikimedia Found. v. NSA*, 857 F.3d 193, 211 (4th Cir. 2017). The court also held that Wikimedia had plausibly alleged standing because it had self-censored its speech and forgone electronic communications in response to Upstream surveillance. *Id*.

The government has moved for summary judgment on standing. In response, Wikimedia has now submitted voluminous evidence establishing that it has standing—and, at the very least, that the government is not entitled to judgment as a matter of law.

Statement of Facts

I. Wikimedia's statement of undisputed material facts

Wikimedia's Internet communications

1. Wikimedia operates twelve free-knowledge Projects on the Internet, including Wikipedia—a free-access encyclopedia that is the Internet's largest and most popular reference work. Wikipedia is one of the top ten most-visited websites in the world. Bayer Decl. ¶ 3 (Pl. Ex. 5). Hundreds of millions of people around the globe use Wikipedia to read or contribute to this immense body of knowledge. *Id.* (more than 1 billion unique device visits per month).

2. Wikimedia engages in more than a trillion international Internet communications each year, with individuals in every country on the planet. *Id.* ¶ 25; Technical Statistics Chart (Pl. Ex. 14). This includes communications between foreign users and Wikimedia's U.S.-based servers, and communications between U.S. users and Wikimedia's foreign servers. Bayer Decl. ¶ 27.

3. Wikimedia's international Internet communications include communications with its community members, internal "log" communications, and staff communications. *See* Paulson Decl. ¶¶ 13-33 (Pl. Ex. 3).

Upstream surveillance of Internet communications

4. For more than a decade, the NSA has used Upstream surveillance to monitor

Americans' international Internet communications. This surveillance involves the NSA's warrantless interception of Internet communications on U.S. soil, in search of communications associated with thousands of individual targets. PCLOB Report 33, 36-41 (Pl. Ex. 15). Although the NSA's targets are foreigners located outside the U.S., this surveillance nonetheless involves the interception and collection of communications belonging to Americans. PCLOB Report 103, 116; [*Redacted*], 2011 WL 10945618, at *27 (FISC Oct. 3, 2011) (Pl. Ex. 16).

5. The government has disclosed a significant amount of information about Upstream surveillance, including dozens of FISC opinions and FISC filings, an exhaustive report by the Privacy and Civil Liberties Oversight Board ("PCLOB"), public testimony by intelligence officials, and official statements by the NSA and Office of the Director of National Intelligence ("ODNI"). *See, e.g.*, PCLOB Report (citing numerous official disclosures); ODNI, *DNI Declassifies Intelligence Community Documents Regarding Collection Under Section 702* (Aug. 21, 2013) (last updated Oct. 11, 2017) (Pl. Ex. 17).

6. To conduct Upstream surveillance, the NSA intercepts communications that transit Internet "backbone" circuits—the "high-speed, ultra-high bandwith" Internet circuits operated by major communication service providers. PCLOB Report 36-37; NSA Resp. to Interrog. No. 12 (Pl. Ex. 18). After taking steps to eliminate wholly domestic traffic, the NSA scans international Internet communications that transit these circuits for "selectors." PCLOB Report 37-41; NSA Resp. to Interrog. Nos. 4, 11. A selector is a communications account, identifier, or address associated with one of the NSA's targets, such as an email address or phone number. May 2, 2011 FISC Submission at 1 (Pl. Ex. 19).

7. In 2017, the NSA targeted more than 129,000 individuals and groups under Section 702. ODNI, *Statistical Transparency Report for Calendar Year 2017* (Apr. 2018) (Pl. Ex. 20).

8. When conducting Upstream surveillance, the NSA cannot know in advance which communications are to, from, or about a targeted selector. PCLOB Report 37; Bradner Decl. ¶ 366(d) (Pl. Ex. 1); *see also* David Kris & J. Douglas Wilson, Nat'l Security Investigations & Prosecutions 2d § 17.5 (2015) ("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." (emphasis in original)). For this reason, Upstream surveillance "may require access to a larger body of international communications than those that contain a tasked selector." PCLOB Report 111 n.476.

9. After scanning communications for selectors, the NSA ingests some communications into its databases for long-term retention. PCLOB Report 111 n.476; Richards Depo. 267:14-19 (ECF No. 143-3). Until April 2017, the NSA ingested communications that were to, from, or "about" a targeted selector. FISC Mem. Op. & Order at 16 (Apr. 26, 2017) (Pl. Ex. 21). 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.

10. The NSA seeks "to comprehensively acquire communications that are sent to or from its targets." PCLOB Report 10, 123. 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." PCLOB Report 143 (emphasis added); *see id.* at 122-23.

11. Upstream surveillance involves the collection of "web activity," June 1, 2011 FISC Submission at 30 (Pl. Ex. 22)—*i.e.*, communications on the "world wide web," which are transmitted using HTTP and HTTPS. Bradner Decl. ¶ 315; Schulzrinne Decl. ¶ 78.

Wikimedia's communications traverse all Internet circuits carrying public Internet traffic into and out of the U.S., including the circuits monitored by the NSA

12. The FISC and the PCLOB have described the locations at which Upstream surveillance occurs based on submissions by Defendants and in documents declassified by them.

According to these disclosures, Upstream surveillance involves monitoring "international Internet link[s]," [*Redacted*], 2011 WL 10945618, at *15, and Internet backbone circuits that facilitate "the flow of communications between communication service providers," PCLOB Report 35-37.

13. Upstream surveillance involves, at a minimum, monitoring high-speed, ultra-high bandwidth circuits that carry Internet traffic between the U.S. and foreign countries. NSA Resp. to Interrog. No. 12; Bradner Decl. ¶¶ 152-53. These circuits are carried on the approximately 50 undersea fiber-optic cables connecting the U.S. and foreign countries, in addition to the terrestrial fiber-optic cables connecting the U.S. with Mexico and Canada. *Id.* ¶ 201. Some of these fiber-optic cables can carry hundreds of "lambdas" or circuits. *Id.* ¶ 206. Nonetheless, the total number of international circuits—or pathways into and out of the U.S.—is small relative to the overall number of Internet circuits. *Id.* ¶¶ 200, 224. These circuits are prime locations to monitor international Internet communications, because the vast majority of Internet traffic between the U.S. and other countries flows over these circuits. *Id.* ¶¶ 220, 222-24.

14. The total volume of Wikimedia's international Internet communications—more than a trillion each year—exceeds, by many orders of magnitude, the number of international Internet circuits connecting the U.S. to other countries. *Id.* ¶¶ 346, 348; *see id.* ¶ 224. Moreover, Wikimedia's communications are broadly distributed, with users in every country. *Id.* ¶¶ 347-48.

15. For these reasons, it is "virtually certain" that Wikimedia's communications traverse every circuit carrying public Internet traffic on every international cable connecting the U.S. to other countries, including the international Internet links monitored by the NSA. *Id.* ¶¶ 6(d), 338, 344-50; *see id.* ¶¶ 331-34.

It is a virtual certainty that the NSA is copying and reviewing some of Wikimedia's trillions of communications in the course of Upstream surveillance

16. Internet communications are split into "packets"—small chunks of information—

as they travel over the Internet. June 1, 2011 FISC Submission at 6; Bradner Decl. ¶¶ 49, 63. Based on the government's detailed descriptions, Upstream surveillance involves these stages: (1) the copying of packets on a circuit; (2) the filtering of the packets to eliminate those that are wholly domestic; (3) the reassembly of the remaining packets into transactions; (4) the review of those transactions for the presence of "selectors"; and (5) the ingestion of transactions that contain selectors into the NSA's Section 702 databases. Bradner Decl. ¶¶ 6(a)-(c), 265-330.

17. The NSA is copying all of the traffic it seeks to review for selectors in one of two ways. The "most likely" means of implementing Upstream surveillance—and the only way in which the NSA could "comprehensively" acquire its targets' communications—is by copying *all* the traffic on the circuits the NSA is monitoring. *Id.* ¶¶ 273-78, 282-83, 289, 335; *see also* PCLOB Report 122-23. If the NSA were *not* seeking to be comprehensive, it could employ an in-line filter to copy only a subset of traffic for monitoring, Bradner Decl. ¶¶ 280-89; but, even then, it is "simply implausible" that the NSA is doing so in a manner that avoids all of Wikimedia's communications, *id.* ¶¶ 7(b), 362, 366-67.

18. For reasons set out in greater detail in the Bradner Declaration, "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), 356.

19. Indeed, when the government's public disclosures about Upstream surveillance are fully considered, the NSA could not comprehensively and reliably collect the communications of its thousands of targets while avoiding all of Wikimedia's communications. *Id.* ¶¶ 6-7, 250-370.

20. The hypothetical scenarios the government's expert offers in explaining how the NSA could avoid all of Wikimedia's international Internet communications are technically inaccurate, ignore critical facts about Upstream surveillance, contradict the government's own

disclosures, and are "simply implausible." *Id.* ¶¶ 357-67, *see also id.* ¶¶ 282-89, 309, 314-15, 326-27, 332-35.

21. Notably, the United Kingdom has publicly acknowledged that—in conducting functionally equivalent surveillance—it is "necessary" to intercept "*all* communications travelling over more than one bearer [circuit] to maximize the chance of identifying and obtaining the communications being sent to known targets." *Case of Big Brother Watch & Others v. United Kingdom*, Eur. Ct. H.R., ¶ 284 (2018) (Pl. Ex. 23); Bradner Decl. ¶¶ 368-69.

The NSA is conducting Upstream surveillance on many international Internet circuits

22. For the preceding reasons, even if the NSA were monitoring only one international Internet link, it is a virtual certainty that the NSA is copying and reviewing some of Wikimedia's communications. Bradner Decl. ¶ 353.

23. In fact, based on the government's official disclosures, Upstream surveillance occurs on multiple circuits. The PCLOB Report repeatedly describes the involvement of multiple "providers," "circuits," and NSA "collection devices." PCLOB Report 7, 12, 35-37, 39-40, 85, 143; *see also* NSA, Dir. of Civil Liberties & Privacy Off. Report 5 (Apr. 16, 2014) ("DCLPO Report") (Pl. Ex. 24); [*Redacted*], 2011 WL 10945618, at *10; Bradner Decl ¶ 353. Moreover, based on the NSA's many targets, the routing patterns of Internet communications, and the fact that targets move over time, Bradner Decl. ¶¶ 309, 333-34, "the NSA is very likely to be monitoring a large number of international circuits, given that it would need to monitor most, if not all, such circuits to accomplish its stated (and unsurprising) goal of reliably and comprehensively collecting the communications of its targets." *Id*. ¶ 353 (emphasis in original).

24. This fact only reinforces the conclusion that some of Wikimedia's many communications are being intercepted, copied, and reviewed by the NSA. *Id.* ¶ 355.

Wikimedia has suffered additional injuries as a consequence of Upstream surveillance

25. Beginning in June 2013, the public disclosures concerning Upstream surveillance and, in particular, the NSA's surveillance of Wikimedia's communications, caused grave concern within the Wikimedia community. Paulson Decl. ¶¶ 40-41; Alexander Decl. ¶ 4 (Pl. Ex. 4).

26. NSA surveillance, including Upstream surveillance, is "highly likely" to have caused the lasting and statistically significant drop in readership of certain Wikipedia pages that began in June 2013, and it has impaired Wikimedia's interactions with its community members. Penney Decl. ¶¶ 10-11 (Pl. Ex. 2); Paulson Decl. ¶¶ 39-47; Alexander Decl. ¶¶ 4-12. In response to Upstream surveillance, Wikimedia has undertaken costly measures to better secure its communications against surveillance and mitigate the threat to its mission. Paulson Decl. ¶¶ 48-59; Alexander Decl. ¶¶ 13-15.

27. Wikimedia enjoys a close and ongoing relationship with its community members, and individual Wikimedia users face clear obstacles to litigating their own rights in this context. Temple-Wood Decl. ¶¶ 8-11, 25-28 (Pl. Ex. 6).

II. Response to Defendants' statement of undisputed material facts

Wikimedia disputes Defendants' statement of material facts as follows:

Paras. 1-6: Denied. These paragraphs do not contain any facts, only legal argument. With respect to paragraph 3, Wikimedia states that the FISC and the PCLOB have described the locations at which Upstream surveillance occurs. *See* Pl. Facts ¶ 12, *supra*.

Paras. 7-8: Denied. As the Bradner Declaration explains, the selective filtering that Schulzrinne hypothesizes is not readily implemented compared to other technical methods, is contradicted by certain government disclosures and rendered "implausible" by others, and would not avoid the interception, copying, and review of all Wikimedia communications. Bradner Decl.

¶¶ 7, 357-70, *see id.* ¶¶ 121-22, 244-47, 250-56, 282-89, 291-94, 298, 312-15, 326-28, 333-35.

Para. 16: Denied. There are a number of circumstances in which IP addresses are not uniquely identifying. *Id.* ¶¶ 244-47, 173-74.

Para. 23: Denied. Not all encryption or implementations of HTTPS in use on the Internet today are "unbreakable." *Id.* ¶¶ 121-22.

Paras. 25-26: Denied on the basis set forth in response to Defendants' paragraphs 7-8.

Paras. 31, 33-37: Denied to the extent the "collector" or "collecting entity" is the NSA conducting Upstream surveillance. Because of the considerable risks to both the provider and the NSA, the NSA is unlikely to engage in any in-line filtering of traffic using whitelists or blacklists—what Schulzrinne calls "traffic mirroring with ACLs"—and it is even less likely to be doing so using complex or sensitive filtering. *Id.* ¶¶ 272-89, 360-67. Moreover, Schulzrinne relies on a premise that has no foundation and "is not remotely possible": the supposition that the NSA knows in advance which IP addresses its targets will use as they move across foreign networks. *Id.* ¶¶ 333, 366(d).

Para. 39: Denied to the extent the "collector" or "collecting entity" is the NSA conducting Upstream surveillance, for the reasons explained in response to Defendants' paragraphs 31, 33-37. Additionally, the NSA has acknowledged relying on telephone numbers as selectors, DCLPO Report 4, collecting "web activity," Bradner Decl. ¶¶ 314-15, and seeking to decipher encrypted communications, *id.* ¶ 326—contradicting Schulzrinne's speculation that, under Upstream, the NSA could collect only emails or would exclude HTTPS communications.

Para. 40: Denied. As the Bradner Declaration explains more generally, if certain traffic is ignored by the NSA, that function is most likely performed by first copying *all* the packets on a circuit, then later filtering out that traffic prior to review. Bradner Decl. ¶¶ 282-89.

Para. 41-42: Denied for the reasons set forth in response to Defendants' paragraphs 31,

33-37. Additionally, the NSA must review all international communications traversing the circuits it is monitoring to "comprehensively" and "reliably" obtain its targets' communications, because the NSA cannot know in advance which communications belong to its targets, or which IP addresses its targets are using. Bradner Decl. ¶ 333. For that reason, "whitelists are almost useless" for Upstream surveillance. *Id.* ¶ 366(d). The whitelisting and blacklisting Schulzrinne hypothesizes also contradict the NSA's concession that it "will acquire" a wholly domestic communication routed over an international Internet link it monitors. *Id.* ¶¶ 292-94.

Para. 43: Denied for the reasons set forth in response to Defendants' paragraphs 7-8.

Paras. 46-47, 49-50: Denied. Selectively filtering to block all packets with port numbers 80 or 443, protocol number 50, or a Wikimedia IP address, is "implausible" in the context of Upstream surveillance; and it would not, as a technical matter, allow the NSA to avoid all of Wikimedia's communications. Bradner Decl. ¶¶ 366-67. The government has also acknowledged that Upstream surveillance involves the collection of "web activity." *Id.* ¶¶ 314-15.

Para. 51: Denied. As the Bradner Declaration explains, when the government's official disclosures about Upstream surveillance are taken into account, it is "implausible" and "basically inconceivable" that the NSA is avoiding the interception, copying, and review of Wikimedia's Internet communications using the methods Schulzrinne hypothesizes. *Id.* ¶¶ 357-67; *see also id.* ¶¶ 282-89.[1]

Argument

I. Wikimedia has standing.

Wikimedia has put forward detailed factual evidence of its injuries, including the copying and review of its communications. This evidence is more than sufficient to defeat the government's motion. Defendants raise only two factual arguments: they argue that Wikimedia

[1] To the extent Defendants' facts are admitted by Wikimedia, they are admitted solely for the purpose of this summary judgment motion.

has presented "no evidence" as to (1) the locations of Upstream surveillance, and (2) the technical basis for concluding that some of Wikimedia's communications are intercepted when they traverse the Internet backbone circuits the NSA is monitoring.[2] Def. Br. 1, 8. On both these questions, however, Defendants' arguments are hollow.

Defendants' first argument shows remarkable disregard for their own public disclosures, because they have declassified information about the locations where Upstream surveillance occurs. In a FISC opinion disclosed by Defendants, the FISC described the NSA's monitoring of communications at "international Internet link[s]," citing Defendants' own court filing. [*Redacted*], 2011 WL 10945618, at *15. Moreover, in a report Defendants have described as exhaustive, the PCLOB explained that Upstream surveillance occurs on Internet backbone "circuits," including those that facilitate "the flow of communications between communication service providers." PCLOB Report 35-37. Having declassified this evidence about the locations where Upstream surveillance occurs, the government cannot now pretend it does not exist.[3]

Defendants' second argument fares no better because their expert declaration opines on the wrong question. Schulzrinne presents a number of hypothetical scenarios, but he offers no opinion whatsoever on the critical factual issue here: the likelihood that the NSA is copying or reviewing some of Wikimedia's trillions of communications in the course of Upstream surveillance. Wikimedia's expert, Scott Bradner, *does* address this question, based on the government's many official disclosures. And in Bradner's exhaustively supported opinion, it is a "virtual certainty" that the NSA is copying and reviewing at least some of Wikimedia's communications as it sifts through Internet traffic to find communications associated with thousands of far-flung targets. Because Defendants do not address the ultimate factual question,

[2] Defendants have not challenged Wikimedia's claim that its communications traverse each international Internet link connecting the U.S. with other countries. Def. Br. 1.

[3] To the extent Defendants are referring to the exact physical locations or facilities where Upstream surveillance occurs, that fact is immaterial. Bradner Decl. ¶ 225.

Wikimedia's evidence on this issue is unrebutted.

Finally, Wikimedia presents evidence that it has suffered additional injuries as a consequence of Upstream surveillance, and those injuries independently support standing.

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 affirmatively show 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, the court may not make credibility determinations but, instead, must accept the nonmoving party's facts as true and draw all reasonable inferences in favor of the nonmoving party. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 255 (1986); *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992).

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). The asserted injury must be "'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Id*. at 158 (quoting *Lujan*, 504 U.S. at 560). Importantly, 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)).[4]

B. As Wikimedia's expert explains, it is a virtual certainty that the NSA is copying and reviewing some of Wikimedia's trillions of Internet communications.

To prevail here, the government must demonstrate that there is no genuine dispute as to a critical fact: whether Wikimedia faces a substantial risk that *any* of its Internet communications will be copied or reviewed under Upstream surveillance. The government cannot possibly satisfy

[4] Standing is evaluated at the time the operative complaint was filed, *see Lujan*, 504 U.S. at 570 n.5, though Wikimedia's evidence shows that its injuries are ongoing.

that burden. As Wikimedia's expert 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). Bradner's conclusion, detailed below, is based on the government's official disclosures and on the expertise he acquired over fifty years of working at Harvard University designing, implementing, and operating large-scale networks. His conclusion and the record upon which it is based are more than sufficient to defeat the government's motion.

Neither the government nor its expert actually addresses the factual question on which Bradner opines—whether the NSA is copying and reviewing any of Wikimedia's communications. The government's expert expresses no opinion whatsoever on that question, and so the only expert conclusion on the critical question here is Bradner's. *See also* Def. Br. 27 ("None of this is to say that the NSA is, in fact, conducting Upstream surveillance using any of these traffic-mirroring techniques, or that using such techniques it is, in fact, blocking all access to Wikimedia's communications.").

Before detailing Bradner's conclusion and his response to the government's expert, Wikimedia addresses one of the government's threshold errors: its mistaken belief that, to demonstrate standing, Wikimedia must disprove every theoretical possibility the government's expert posits for how Upstream surveillance could be conducted. That is not Wikimedia's burden, not even at trial. The Fourth Circuit found Wikimedia's allegations plausible, but it did not, as the government appears to suggest, fundamentally alter the factual question at issue: whether it is likely that the NSA is copying or reviewing some of Wikimedia's communications? On that question, there is only one expert opinion—"yes."

1. Based on the government's official disclosures, it is virtually certain that the NSA is copying and reviewing at least some of Wikimedia's trillions of Internet communications.

Based on the government's disclosures about Upstream surveillance and based on the volume and distribution of Wikimedia's communications, Scott Bradner, an Internet networking expert, has concluded 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." Bradner Decl. ¶ 6(e).[5] His conclusion flows from three essential points.

First, "it is virtually certain that Wikimedia's international communications traverse every circuit carrying public Internet traffic on every international cable connecting the U.S. to other countries." Bradner Decl. ¶ 6(d). In other words, Wikimedia's international communications travel on every possible Internet path into and out of the country. This is due to the volume and global distribution of Wikimedia's communications and the relatively few international circuits connecting the U.S. to other countries.

Wikimedia's international Internet communications are immense in volume and global in distribution. As the operator of one of the ten most-visited websites in the world, Wikimedia engages in more than a trillion international Internet communications each year. *Id*. ¶¶ 339, 346. Wikimedia operates webpages in 288 languages, and its trillions of communications reach hundreds of millions of users, spread throughout every country on Earth. *Id.* ¶¶ 341, 346-47. At

[5] 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 (LMAnet) and the New England Academic and Research Network (NEARnet). 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, as well the IETF's general management committee, the Internet Engineering Steering Group. Bradner served as Harvard University's Chief Technology Security Officer for a number of years. Most recently, Bradner worked with identity management and enterprise architecture.

the same time, the Internet circuits connecting the U.S. to the rest of the world are few in number compared to the volume of Wikimedia's communications, and those circuits arrive at natural chokepoints. *Id.* ¶¶ 200-18, 222-24. There are about 50 undersea fiber optic cables and relatively few terrestrial cables connecting the U.S. to other countries. *Id.* ¶¶ 201-05, 224. These cables, in the aggregate, carry thousands of circuits, *id.* ¶ 228, and "essentially all of the public Internet communications between the U.S. and other countries flow over these circuits." *Id.* ¶ 222.

Based on the volume and distribution of Wikimedia's international Internet communications and the relatively few circuits connecting the U.S. to the rest of the world, Bradner concludes that it is "virtually certain" that Wikimedia's communications traverse each of those circuits. *Id.* ¶¶ 336-38, 341-50; *id.* ¶ 348 ("[E]ven if there are thousands of international circuits, there would still be hundreds of millions of Wikimedia communications on the average circuit.").

Second, the government has acknowledged conducting Upstream surveillance on at least one "international Internet link." *Id*. ¶¶ 291-92 (quoting [*Redacted*], 2011 WL 10945618, at *15). 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. *Id.* ¶ 225. 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. PCLOB Report 37-38 & n.140.

In fact, the government has publicly acknowledged that, in the course of Upstream surveillance, the NSA monitors *multiple* circuits. *See* Pl. Facts ¶ 23, *supra*.

Third, the NSA could not conduct Upstream surveillance as it has described it without copying, reassembling, and reviewing all international communications traversing each circuit it

is monitoring. Thus, the government would be copying and reviewing Wikimedia's communications even if it were monitoring only a single circuit.

The government has said that it attempts through Upstream surveillance "to *comprehensively acquire* communications that are sent to or from its targets," PCLOB Report 10, 123, 143 (emphasis added), but it could not do so without first copying essentially all international communications going over the circuits it is monitoring. This is because, as a technological matter, the NSA could not identify all of the communications of its targets crossing a circuit it is monitoring *without* reviewing all international communications crossing that circuit for the presence of selectors. And it could not review those communications for selectors without first copying and reassembling them. In short, to comprehensively acquire the communications of its targets, the NSA must be comprehensively copying, reassembling, and reviewing the international communications on the circuits it is monitoring. As Bradner summarizes it:

> [I]f the NSA's goal is to comprehensively obtain its targets' communications, then it must comprehensively copy, reassemble and review all transactions that could conceivably be to or from a target that transit the circuits being monitored. Since all transactions transiting the monitoring points other than the ones that are wholly domestic could be to or from a target, the NSA must be copying, reassembling and reviewing all, or essentially all, international transactions that transit the circuits being monitored.

Bradner Decl. ¶ 335.

The government's own disclosures indicate that the NSA is in fact reviewing all communications on the international circuits it monitors. For example, in a submission to the FISC, "the government readily concede[d] that NSA *will acquire* a wholly domestic 'about' communication if the transaction containing the communication is routed through an international Internet link being monitored by NSA." [*Redacted*], 2011 WL 10945618, at *15 (emphasis added); *see id.* at *11 ("NSA's upstream collection also acquires . . . *any* Internet transaction that references a targeted selector . . . ." (emphasis added)). This concession would be

accurate only if the NSA were copying, reassembling, and reviewing *all* communications on the international circuits it is monitoring. Bradner Decl. ¶¶ 293-94. The PCLOB has described the breadth of Upstream surveillance in similar terms. PCLOB Report 122 (analyzing Upstream surveillance based on the government's use of technology that allows it "to examine the contents of *all* transmissions passing through collection devices and acquire those, for instance, that contain a tasked selector anywhere within them" (emphasis added)).

Bradner explains in detail why the NSA must—as a matter of technological necessity—copy, reassemble, and review all communications on the international circuits it monitors, if it wishes to acquire all of the communications of its targets. Bradner Decl. ¶¶ 236-48, 301-14, 333, 335. The critical point is that the NSA cannot know, as each packet crosses a circuit it is monitoring, whether that packet belongs to a transaction containing a selector. *See, e.g.*, *id.* ¶ 333 ("[T]he NSA must be comprehensively reviewing Internet transactions to see if they are transactions to or from NSA targets, since the NSA cannot know in advance which of the many transactions on the Internet could be to or from one of the NSA's targets."). The reason the NSA cannot know is that the selectors it uses to identify its targets' transactions appear within the "application layer" of the packets, which the NSA cannot review for selectors without first copying and reassembling each transaction. *Id.* ¶¶ 301-09 (explaining that Upstream surveillance requires "reassembly" of communications for review); *id.* ¶¶ 310-18; *see also* Richards Depo. 263:11-18. In other words, because the NSA cannot know which packets are part of a transaction containing a selector without first copying, reassembling, and reviewing that transaction, the NSA must review all international transactions on each circuit it monitors to comprehensively acquire its targets' transactions. Bradner Decl. ¶¶ 333, 335.

Even setting aside the technological reasons why the NSA must be copying and reviewing Wikimedia's communications to acquire its targets' communications, there are other

compelling reasons to conclude that the NSA is copying all communications—including Wikimedia's—on the circuits it is monitoring. Bradner explains that, to conduct Upstream surveillance, the NSA must first copy those Internet packets constituting the transactions it will review for selectors. *Id.* ¶ 272. As a technical matter, there are only two possible ways in which the NSA could be carrying out that copying. *Id.* First, the NSA could be copying *all* of the packets on any given circuit it is monitoring—by, for example, using a fiber-optic splitter—before sending the duplicated stream of traffic to a filter (if necessary). *Id.* ¶¶ 272(a), 273-79; *see* Schulzrinne Decl. ¶ 55. Second, the NSA could be utilizing an "in-line filter" to copy only those packets that satisfy certain criteria. Bradner Decl. ¶¶ 272(b), 280-81; *see* Schulzrinne Decl. ¶ 57. These two possible configurations are depicted in Figures 33 and 36 of the Bradner Declaration.

Bradner explains that the NSA is most likely using the copy-then-filter configuration. Bradner Decl. ¶¶ 282-89. Using the copy-then-filter configuration would permit the NSA to conduct Upstream surveillance without disclosing its filtering criteria to Internet service providers, leaving "the NSA in full control of the upstream collection process." *Id.* ¶ 283. In contrast, "the in-line filter configuration would require either that [an Internet service provider] agrees to place an NSA-operated device into the heart of its network," or that the NSA disclose its filtering criteria to the Internet service provider's personnel to operate the filter. *Id.* ¶ 284. Neither is likely. The first risks interfering with the Internet service provider's ordinary network operations, *id.* ¶¶ 284, 289, and the second "would require that [Internet service provider] personnel know what the NSA's filter criteria were," *id.* ¶ 285. As Bradner summarizes: "the copy-then-filter configuration gives the NSA the greatest operational control and confidentiality in carrying out upstream collection with the least risk of interference with the [provider's] ordinary network operations." *Id.* ¶ 289; *see* 50 U.S.C. § 1881a(i)(1)(A) (authorizing the government to compel assistance "in a manner that will protect the secrecy of the acquisition and

produce a minimum of interference" with the company's service).

Bradner's conclusions are corroborated by descriptions of two similar surveillance programs. The U.S. government, for instance, operates another program of "deep packet inspection" known as EINSTEIN 2, which involves the monitoring of Internet circuits to detect attacks on government networks. *See id.* ¶ 259 (explaining that Upstream surveillance is a form of deep packet inspection). Like Upstream, it involves copying entire streams of traffic, in part to avoid "disrupt[ing] the normal operations of [the systems being monitored]."[6] *See id.* ¶¶ 283-87.

More recent disclosures by the United Kingdom also corroborate Bradner's conclusions. *See id.* ¶¶ 368-69. The U.K.'s counterpart to the NSA—the GCHQ—recently disclosed that in the course of functionally equivalent surveillance, it must also intercept the entire stream of communications on any circuit it monitors: "For 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." *Id.* ¶ 368 (quoting Further Observations of the Government of the United Kingdom ¶¶ 7-8, *10 Human Rights Organisations v. United Kingdom*, Eur. Ct. H.R. (Dec. 16, 2016)).

For these reasons, it is virtually certain that the NSA has copied and reviewed at least some of Wikimedia's trillions of communications.[7]

2. The government's expert declaration is flawed and does not address the question of whether the NSA is copying and reviewing Wikimedia's communications.

The government's expert, Dr. Henning Schulzrinne, postulates a manner of conducting

[6] *See Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection System (Einstein 2.0)* 33 Op. O.L.C. 1, 4 (Jan. 9, 2009) (Pl. Ex. 25) ("EINSTEIN 2.0 sensors will not scan actual Federal Systems Internet Traffic for malicious computer code as that traffic is in transmission, but instead will scan a temporary copy of that traffic created solely for the purpose of scanning by the sensors.").

[7] For purposes of standing, it is sufficient that the NSA is copying Wikimedia's communications.

"Upstream-*type* surveillance," Schulzrinne Decl. ¶¶ 15, 53, 77, 88 (emphasis added), that bears almost no relationship to the government's stated purposes in conducting Upstream surveillance and that reflects little familiarity with the government's own disclosures. As detailed below, Schulzrinne's declaration fails to "mention many of the critical features of upstream collection on which [Bradner] base[s] [his] conclusion that it is a virtual certainty that the NSA has copied, reassembled or reviewed at least some of Wikimedia's communications." Bradner Decl. ¶ 358. Remarkably, Schulzrinne also fails to express any opinion whatsoever on the most critical question at this stage: is it likely that the NSA is copying or reviewing any of Wikimedia's communications in the course of Upstream surveillance? Schulzrinne studiously avoids answering that question, just as he conspicuously avoids opining on the likelihood that his technical hypotheticals reflect the NSA's actual practices. For that reason, Schulzrinne's hypothetical conjectures are immaterial and should be rejected.[8] In any event, his speculations are technically inaccurate on a central point, and they are—given what the government has acknowledged about Upstream surveillance—"simply implausible." *Id.* ¶ 362.

Schulzrinne first suggests that the NSA could utilize an in-line filter to engage in "whitelisting" or "blacklisting" of monitored traffic, so as to avoid copying *all* communications transiting circuits on which it conducts Upstream surveillance, Schulzrinne Decl. ¶¶ 57, 73-76, but Schulzrinne ignores critical disclosures about Upstream that make this conjecture pure fantasy. He ignores the government's acknowledgment that Upstream surveillance is designed "to *comprehensively acquire* communications that are sent to or from its targets," PCLOB Report 10, 123, 143 (emphasis added), which the NSA could not do without copying and reviewing essentially all international communications on the circuits it is monitoring. He ignores the

[8] Indeed, in similar circumstances, in which an expert's testimony focuses on generalized evidence or distant hypotheticals divorced from the factual record of the case, courts have rejected that testimony. *See United States v. Ancient Coin Collectors Guild*, 899 F.3d 295, 319 (4th Cir. 2018); Fed. R. Evid. 702(d).

government's "conce[ssion] that NSA *will acquire* a wholly domestic 'about' communication if the transaction containing the communication is routed through an international Internet link being monitored by NSA," [*Redacted*], 2011 WL 10945618, at *15 (emphasis added), which would have been a misrepresentation rather than a concession if the NSA were not copying and reviewing all communications on international circuits it monitors. Bradner Decl. ¶¶ 293-94. And he ignores the compelling practical reasons that the NSA is most likely not using an in-line filter at all, given the significant advantages of using the copy-then-filter configuration and the significant risks of using an in-line configuration. *Id*. ¶¶ 282-89, 363-65.

The specific forms of "whitelisting" and "blacklisting" that Schulzrinne postulates are even more fanciful. Schulzrinne first says the NSA could be "whitelisting" IP addresses associated with its targets, Schulzrinne Decl. ¶ 65, but as Bradner explains, "whitelists are almost useless for the type of collection program the NSA is running." Bradner Decl. ¶ 366(d). "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," *id.*, particularly given that the NSA has over 129,000 targets under Section 702. ODNI Statistical Transparency Report 14. Schulzrinne's suggestion of whitelisting IP addresses also ignores the NSA's "about" collection of communications that are neither to nor from its targets—and which therefore cannot be identified by their IP addresses as belonging to a target. And more broadly, it ignores the NSA's reliance on selectors that do not appear in the addressing information of packets, such as email addresses, which appear only in the so-called "application layer." Bradner Decl. ¶¶ 312-14.

Schulzrinne next suggests that the NSA could be "blacklisting" all "web communications," Schulzrinne Decl. ¶ 79, but this directly contradicts the government's representation to the FISC of "Section 702 upstream collection of web activity." June 1, 2011

FISC Submission at 30; *see* Bradner Decl. ¶¶ 314-15, 366(f). Excluding web communications would, moreover, "leave a very large hole in the NSA's collection ability." *Id.* ¶ 366(f). The web—that is, HTTP and HTTPS—transports some of the most common Internet communications: "web email, web chat, web-based editors which have been used to send hidden messages, ISIS videos and the like." *Id.* It beggars belief to suggest that a program designed "to comprehensively acquire" the Internet communications of the NSA's targets would be designed to ignore the most common of those communications. More generally, blacklisting any particular Internet application or port, as Schulzrinne posits, "would create a blind spot" that sophisticated targets "could easily probe to find . . . and exploit." Bradner Decl. ¶ 366(b).

Next, Schulzrinne says that the NSA might be "blacklisting" HTTPS and IPSec communications because they are encrypted, Schulzrinne Decl. ¶¶ 71, 79, 84, but this ignores the permission the FISC has granted the NSA to retain "all communications that are enciphered or reasonably believed to contain secret meaning," and to attempt to decrypt that material. NSA Section 702 Minimization Procedures § 5(3) (2014) (Pl. Ex. 26). Schulzrinne also ignores the "obvious reasons that the NSA would seek to collect traffic on port 443 even though it is encrypted," Bradner Decl. ¶ 326, and the similar "incentive[s it would have] to collect encrypted communications of all types," *id.* ¶ 328, including (1) the fact that revealing metadata can be obtained from encrypted communications even if they cannot be decrypted, *id.* ¶ 326(c), and (2) the possibility that the NSA may be able to compromise the encryption now or in the future, as its procedures specifically contemplate, *id.* ¶¶ 121-22, 326(a)-(b), among other reasons, *see id.* ¶¶ 326**,** 366(b), (f)-(g).[9]

Finally, Schulzrinne suggests that the NSA could have "blacklisted" Wikimedia's IP

[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).

addresses, Schulzrinne Decl. ¶ 80, but as Bradner explains, this is "inconceivable." Bradner Decl. ¶ 367(a). There are millions of websites on the public Internet, and the notion that "NSA would have gone through them to decide which to monitor and which not to" is, as Bradner concludes, "totally unbelievable." *Id.* Doing so would also needlessly ignore "a potentially valuable source of information about the online research and reading of [the NSA's] targets" on Wikimedia's websites. *Id.* Schulzrinne says the NSA might "blacklist" Wikimedia's IP addresses to reduce the volume of data for processing, Schulzrinne Decl. ¶ 79, but Bradner explains that this makes little sense. "[D]eep packet inspection devices . . . can process or review Internet communications at the same rate that those communications traverse high-bandwidth Internet links." Bradner Decl. ¶ 288. And if the NSA wanted to monitor less traffic, it would be far preferable to "blacklist" video traffic rather than Wikimedia traffic. *Id.* ¶ 366(c).

Schulzrinne is also technologically wrong on a point important to his conjecture. He claims that, if the NSA "blacklisted" Wikimedia's IP addresses, "the NSA would receive no access to . . . Wikimedia communications of any kind." Schulzrinne Decl. ¶ 81. This is incorrect. Bradner Decl. ¶ 367(b). Even if the NSA "blacklisted" Wikimedia's IP addresses, it would nevertheless copy and review Wikimedia communications in at least three circumstances: (1) when a so-called "multi-communication transaction" contains a Wikimedia communication, (2) when an email to or from Wikimedia transits a circuit being monitored by the NSA during the leg in its multi-hop journey where it does not have a Wikimedia IP address associated with it, and (3) where Wikimedia communications pass through a tunnel (or "virtual private network"), such that they would not have a Wikimedia IP address in their addressing information. *See id.*

For these reasons and others set out in his declaration, Bradner concludes that Schulzrinne's speculations are "simply implausible." *Id.* ¶ 362.

C. Wikimedia has suffered additional injuries that establish its standing.

Wikimedia has suffered additional injuries as a consequence of Upstream surveillance that independently establish its standing. First, Upstream surveillance has impaired Wikimedia's communications with its community members in several ways, including a steep and lasting drop in the readership of certain Wikimedia pages. Second, in response to Upstream surveillance, Wikimedia has taken protective measures to mitigate the NSA's intrusions.

Beginning in June 2013, there were a series of public disclosures in the press and by the government concerning the existence, scope, and operation of Upstream surveillance. *See* PCLOB Report. Among the disclosures in the press, *The Guardian* newspaper and others published multiple NSA slides showing that the NSA was surveilling Wikimedia's communications to obtain intelligence information. One of the published NSA slides described analysts' ability to learn "nearly everything a typical user does on the Internet" by surveilling HTTP communications—and identified Wikipedia as a prime example of the HTTP communications collected through NSA surveillance. Pl. Ex. 28.[10] Another NSA slide published in July 2015 similarly showed that the NSA was intercepting Wikimedia's communications and had designed software to allow analysts to identify those communications in NSA databases. Pl. Ex. 30 (slide 9).[11] These disclosures caused grave concern within the Wikimedia community and among Wikimedia staff. Paulson Decl. ¶¶ 40-41; Alexander Decl. ¶ 4.

1. Upstream surveillance has impaired Wikimedia's activities and ability to communicate with its community members.

NSA surveillance, including Upstream surveillance, has caused a lasting and statistically significant drop in readership of certain Wikipedia pages, as illustrated by Dr. Jonathon Penney's

[10] *See* Glenn Greenwald, *XKeyscore: NSA Tool Collects "Nearly Everything a User Does on the Internet*," Guardian, July 31, 2013 (Pl. Ex. 27).

[11] The slide shows NSA code used to identify "wikipedia" and "wikimedia" communications. *See* Morgan Marquis-Boire, *et al.*, *XKEYSCORE*, Intercept, July 1, 2015 (Pl. Ex. 29).

empirical study of years' worth of Wikipedia pageview data. Penney Decl. ¶¶ 10-11. Following a comprehensive statistical analysis, Penney concludes that increased public awareness in June 2013 of NSA surveillance, including Upstream surveillance, is highly likely to have caused the sharp and sustained drop in readership of certain terrorism-related Wikipedia articles after the June 2013 revelations. *Id.* ¶ 10-11, 22-58.

This broad harm to Wikimedia has been palpable, also, in many of Wikimedia's interactions with its community members. Following the disclosures in 2013, Wikimedia received dozens of complaints regarding Upstream surveillance and held community-wide consultations that addressed the impact of NSA surveillance. Alexander Decl. ¶ 4; Paulson Decl. ¶¶ 46, 58. NSA surveillance, including Upstream surveillance, has driven community members to self-censor their speech or limit their engagement with Wikimedia. Alexander Decl. ¶¶ 4-12; Paulson Decl. ¶¶ 43-47. Likewise, Wikimedia staff have self-censored their speech and at times forgone electronic communications. Alexander Decl. ¶¶ 13-16; Paulson Decl. ¶¶ 48, 57.

These harms constitute concrete injuries-in-fact that are directly traceable to Upstream surveillance. Indeed, the Fourth Circuit has already held that "because Wikimedia has self-censored its speech and sometimes forgone electronic communications in response to Upstream surveillance, it . . . has standing to sue for a violation of the First Amendment." *Wikimedia*, 857 F.3d at 211. While "[a]llegations of a subjective 'chill' are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm," *Amnesty*, 568 U.S. at 418 (quoting *Laird v. Tatum*, 408 U.S. 1, 10-15 (1972)), the injuries to Wikimedia's protected activities are specific, objective, and concrete. Unlike in *Laird*, Wikimedia challenges warrantless surveillance of private communications, and it has presented extensive evidence of the measurable harms that have resulted from Upstream surveillance. *See* Penney Decl.; Alexander Decl.

2. Upstream surveillance has required Wikimedia to take costly protective measures.

In response to Upstream surveillance and NSA surveillance of Wikimedia's communications, Wikimedia has undertaken expensive and time-consuming measures to protect its users and communications, including (1) transitioning all of Wikimedia's webpages from HTTP to HTTPS-by-default; (2) implementing Internet Security Protocol; (3) acquiring new technical infrastructure; and (4) hiring a full-time engineer to manage these efforts. Paulson Decl. ¶¶ 48-59. Together, these measures required several years' worth of employee work and more than $300,000. *See id.* Wikimedia has also made costly changes to its staff's modes of communication with community members, many of whom have refused to communicate with Wikimedia via email. Alexander Decl. ¶¶ 6, 9, 13-15.

Because these protective measures constitute concrete injuries that are fairly traceable to Upstream surveillance, they confer standing. In *Amnesty*, the Supreme Court recognized that a plaintiff may establish standing by showing that it took protective measures to mitigate harm. *See* 568 U.S. at 414 n.5. Although the plaintiffs in *Amnesty* had taken such steps, the Court concluded that the measures were insufficient because the risk of surveillance was a "hypothetical future harm." *Id.* at 416. Here, however, the harm that Wikimedia faces from Upstream surveillance is well-established. *See Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 153 & n.3 (2010). Wikimedia has not challenged a hypothetical program of narrowly targeted surveillance, but rather an acknowledged form of surveillance that involves the systematic copying and review of international Internet communications.

D. Wikimedia has third-party standing to assert the rights of its users.

Wikimedia has third-party standing to assert the rights of (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.[12] Wikimedia satisfies all three conditions for third-party standing. *See Kowalski v. Tesmer*, 543 U.S. 125, 129-30 (2004). First, Wikimedia itself has stated an injury-in-fact based on the interception of its communications and other injuries above. Second, Wikimedia enjoys a close and ongoing relationship with many of the community members whose rights it seeks to protect, and thus it will be an effective proponent of those users' rights. Paulson Decl. ¶¶ 8-12; Temple-Wood Decl. ¶¶ 8-11. Finally, these parties face clear obstacles to litigating their own rights, including the risk to their anonymity. Temple-Wood Decl. ¶¶ 18-28.

II. The government's state secrets arguments are meritless.

The government advances two sweeping claims about the operation of the state secrets privilege in this case. Both are at odds with this Court's prior ruling and should be rejected.

Throughout its brief, the government contends that because the Court refused to compel the production of certain documents based on the state secrets privilege, the Court is barred from considering the government's own *public* disclosures to determine whether Wikimedia "is or was subject to Upstream surveillance activities." *See* Def. Br. 1-2, 7, 21-23, 29 (urging that official disclosures be "removed from the case" entirely). That argument fails on several grounds.

First, the Court has already ruled that Wikimedia is entitled to show that its communications are being copied and reviewed based on this public evidence, and thus it has already rejected the government's argument here. *See Wikimedia Found. v. NSA*, 2018 WL 3973016, at *8 (D. Md. Aug. 20, 2018) ("courts have recognized that plaintiffs can 'rely on many non-classified materials, including present and future public disclosures of the government

[12] Like Wikimedia itself, users in the first and second categories face a substantial likelihood that their communications will be subject to Upstream surveillance. *See* Bradner Decl. ¶¶ 353-54; Technical Statistics Chart (2.8 billion requests from U.S. users to Wikimedia servers abroad).

or [telecommunications providers] on the alleged NSA programs'" to establish that they have been subject to surveillance (citation omitted)).

Second, application of the state secrets privilege in response to a motion to compel simply removes particular pieces of evidence from the case. It does not foreclose all litigation on a topic, precisely because other sources of evidence are often available. *See United States v. Reynolds*, 345 U.S. 1, 11 (1953).

Third, the state secrets privilege depends on a showing of reasonable danger that disclosure would harm national security, *see id.* at 7-8, 10, and no harm can come from the Court's consideration of evidence that the government has chosen to publicly disclose. *See Abilt v. CIA*, 848 F.3d 305, 312 (4th Cir. 2017) (courts review state secrets claims with "a skeptical eye"). The government's new claim is wholly distinct from any risk arising from the disclosure of specific *classified* documents, which was the subject of Defendants' prior state secrets invocation. Moreover, in ruling on the government's motion, this Court is not ruling on whether Wikimedia "is or was subject to Upstream surveillance." Def. Br. 29. Rather, the Court is assessing whether there is a genuine dispute of material fact with respect to Wikimedia's claim that its communications are, at a minimum, at *substantial risk* of being copied and reviewed.

The government's other claim about the operation of the state secrets privilege fails for similar reasons. It contends that even if Wikimedia could demonstrate a genuine issue of material fact concerning standing, the litigation "cannot proceed" due to the "risk of disclosing privileged information." Def. Br. 29. Defendants do not explain what privileged information would be placed at risk, or how, given that the litigation is presently confined to the extensive public record. But in any event, Congress anticipated and addressed this very risk in FISA. To the extent that sensitive information is implicated by future proceedings in this case, FISA's procedures expressly authorize the Court to review such materials in camera, just as this Court

has regularly done in criminal cases involving FISA. 50 U.S.C. § 1806(f).[13] None of the cases Defendants cite involved FISA surveillance, and thus FISA's mandatory in camera review procedures were simply unavailable. *See Sterling v. Tenet*, 416 F.3d 338 (4th Cir. 2005); *Abilt*, 848 F.3d 305.[14]

Ultimately, the government is arguing that it alone may dictate who can challenge FISA surveillance, regardless of what the non-classified evidence shows. Both Congress and this Court have rejected that argument. Indeed, Congress enacted FISA's procedures precisely so that surveillance challenges like this one could be heard by the courts. *See* H.R. Rep. No. 95-1720 at 31-32 (1978) ("an in camera and ex parte proceeding is appropriate . . . in both criminal and civil cases"); *Wikimedia*, 2018 WL 3973016, at *8 ("affirmative government acknowledgement of surveillance of a specific target is not the only means by which a plaintiff can establish evidence of his or her 'aggrieved person' status").

Conclusion

For the reasons above, Defendants' motion should be denied.

[13] Even if a plaintiff must establish a genuine dispute of material fact concerning its status as an "aggrieved person" before invoking FISA's procedures, Wikimedia has done so here. *Wikimedia*, 2018 WL 3973016, at *8 ("to trigger § 1806(f) procedures, a plaintiff must first adduce evidence sufficient at least to create a genuine dispute" as to whether the plaintiff is or was subject to surveillance).

[14] It bears emphasis that the Court's in camera review would be greatly simplified, because it would include direct evidence of the interception of Wikimedia's communications.

Dated: December 18, 2018

Respectfully submitted,

/s/ David R. Rocah
David R. Rocah (Bar No. 27315)
Deborah A. Jeon (Bar No. 06905)
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

/s/ Patrick Toomey
Patrick Toomey (pro hac vice)
(*signed by Patrick Toomey with permission of David R. Rocah*)
Ashley Gorski (pro hac vice)
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

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

Counsel for Plaintiff

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