IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, Plaintiff, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	Civil Action No. 1:15-cv-00662-TSE

Attachment A

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, Plaintiff, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	No. 1:15-cv-0662 (TSE) ~~FILED UNDER SEAL~~

BRIEF IN SUPPORT OF DEFENDANTS' MOTION FOR SUMMARY JUDGMENT

Dated: November 13, 2018

JOSEPH H. HUNT
Assistant Attorney General

ANTHONY J. COPPOLINO
Deputy Branch Director

JAMES J. GILLIGAN
Special Litigation Counsel

RODNEY PATTON
Senior Trial Counsel

JULIA A. BERMAN
Senior Counsel

OLIVIA HUSSEY SCOTT
Trial Attorney

U.S. Department of Justice
Civil Division, Federal Programs Branch
1100 L Street, N.W., Room 11200
Washington, D.C. 20005
Phone: (202) 514-3358
Fax: (202) 616-8470
Email: james.gilligan@usdoj.gov

Counsel for Defendants

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES

CASES **PAGE(S)**

PAGE(S)

STATUTES

RULES

MISCELLANEOUS

INTRODUCTION

A one-legged stool cannot stand. And that is what has become of Plaintiff Wikimedia Foundation's tripartite theory that the National Security Agency ("NSA"), in the course of conducting Upstream surveillance, "must be" intercepting, copying, and reviewing at least some of Wikimedia's international online communications. Of the three essential allegations that must be proven (at the least) to establish Wikimedia's standing to contest the legality of Upstream surveillance, Plaintiff has adduced no admissible evidence to support two of them. Furthermore, undisputed expert testimony demonstrates that one of those two allegations, concerning "technical rules of how the Internet works," *Wikimedia Found. v. NSA*, 857 F.3d 193, 210 (4th Cir. 2017), is not only unsupported, it is simply wrong.

When the Fourth Circuit heard this case, it held that Wikimedia had plausibly alleged its standing based on three "key" allegations: (i) that its communications almost certainly traverse every "international backbone link" between the United States and the rest of the world; (ii) that the NSA is conducting Upstream surveillance at one or more of these "international Internet links"; and (iii) that at any such link where the NSA conducts Upstream surveillance, as a technical matter, it "must be" copying and reviewing all international text-based communications transiting that link in order to "reliably" obtain communications to or from its intelligence targets.

Plaintiff has no proof, however, of the second allegation, that the NSA conducts Upstream surveillance at one or more "international Internet links." Indeed, the location(s) and nature of the site(s) at which the NSA conducts Upstream surveillance is a fact over which the Government has asserted the state secrets privilege, an assertion this Court has upheld, thus removing all evidence of where Upstream surveillance is conducted from the case. Without such evidence, Plaintiff cannot establish that Upstream surveillance occurs at Internet backbone links that its communications transit, or, therefore, that its communications have been or will be intercepted, copied, or reviewed by the NSA in the course of that surveillance.

Plaintiff also has adduced no evidence to support its third essential allegation, that the NSA, as a technical matter, "must be" copying and reviewing all communications (and, hence, Wikimedia's) transiting any given international backbone link it monitors. Whether or not the NSA in fact copies and reviews all communications transiting the location(s) where Upstream surveillance takes place is also a classified operational detail subject to the Government's valid claim of privilege. Therefore, all evidence of that fact, too, is removed from the case. In any event, undisputed expert testimony presented by the Government shows that this essential allegation is, as a technical matter, simply mistaken. There are a number of technically feasible, readily implemented means by which Upstream surveillance could be conducted at any given Internet backbone "link" without intercepting, copying, or reviewing Wikimedia's communications.

Thus, like any one-legged stool must do, Wikimedia's theory of standing collapses, and judgment must be awarded to the Defendants as a matter of law.

Even if there were a genuine issue of material fact as to all three essential elements of Plaintiff's standing theory, a trial of these facts could not go forward, because it would present an unacceptable risk of disclosing privileged state secrets concerning Upstream surveillance. Indeed, "the whole object of the [adjudication] . . . [would be] to establish a fact that is a state secret," *Sterling v. Tenet*, 416 F.3d 338, 348 (4th Cir. 2005)—whether Plaintiff's communications have been or will be subject to Upstream surveillance. Under the binding law of this Circuit, such a case cannot proceed.

BACKGROUND

Upstream Collection Under Section 702 of the Foreign Intelligence Surveillance Act

As this Court is already aware, Congress enacted Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1881a, in 2008 to address intelligence-collection challenges that had arisen from fundamental changes in communications technology since FISA's original enactment in 1978. *See Wikimedia Found. v. NSA*, 143 F. Supp. 3d 344, 347-48 (D. Md. 2015); *see also Clapper v. Amnesty Int'l, USA*, 568 U.S. 398, 403-04 (2013). Section 702 permits the Attorney General

and the Director of National Intelligence ("DNI") to jointly authorize, for up to one year, foreign-intelligence surveillance targeted at non-U.S. persons located abroad, without regard to the location of the collection, upon approval by the Foreign Intelligence Court ("FISC") of a "certification," submitted by the Government, demonstrating that the intended surveillance complies with the statute's various requirements and limitations. 50 U.S.C. § 1881a(a), (b), (h), (j); *Amnesty Int'l*, 568 U.S. at 404; *Wikimedia Found. v. NSA*, 857 F.3d 193, 201 (4th Cir. 2017).

After the FISC approves a § 702 certification, NSA analysts identify non-U.S. persons located outside the United States who are reasonably believed to possess or receive, or are likely to communicate, foreign-intelligence information designated in the certification. *See* Privacy & Civil Liberties Oversight Board Report on the Surveillance Program Operated Pursuant to Section 702 of the FISA ("PCLOB 702 Report"), at 41-46, https://www.pclob.gov/library/702-Report.pdf. Once the NSA has designated a target, it then attempts to identify specific means by which the target communicates, such as an e-mail address or a telephone number, which is referred to as a "selector." NSA Director of Civil Liberties and Privacy Office Report, NSA's Implementation of FISA Section 702, at 4, https://www.nsa.gov/Portals/70/documents/about/civil-liberties/reports/nsa_report_on_section_702_program.pdf. Selectors may not be key words or the names of targeted individuals, but must be specific communications identifiers. *Id.*; PCLOB 702 Report, at 32–33, 36. To effect acquisition, the Government may issue a § 702 "directive" to a U.S. telecommunications-service provider requiring it to assist the Government in acquiring communications involving those selectors. 50 U.S.C. § 1881a(i); PCLOB 702 Report, at 32–33.

Upstream Collection

The Government has acknowledged conducting two forms of surveillance under § 702, so-called PRISM collection, and Upstream surveillance. Only Upstream is at issue in this case. *See* First Amended Complaint, ECF No. 72 ("Am. Compl.") ¶¶ 39-40.

Although the Upstream collection process has been described in general, unclassified terms in declassified documents and unclassified reports, certain operational details remain highly classified and, as this Court recently held, are subject to the state secrets privilege. *See Wikimedia Found. v. NSA*, 2018 WL 3973016, at *10-14 (D. Md. Aug. 20, 2018). In unclassified terms, in the course of Upstream collection "certain Internet transactions transiting the Internet backbone network(s) of certain electronic communication service provider(s) are filtered for the purpose of excluding wholly domestic communications[,] and are then scanned to identify for acquisition those transactions [that contain communications] to or from . . . persons targeted in accordance with the applicable NSA targeting procedures; only those transactions that pass through both the filtering and the scanning are ingested into Government databases." Pub. Decl. of Daniel R. Coats, DNI, ECF No. 138-2 ("DNI Decl.") ¶ 15; *see also* PCLOB 702 Report, at 37.[1]

Plaintiff's Allegations

Plaintiff Wikimedia Foundation, along with eight other organizations and associations, brought this action alleging that Upstream surveillance exceeds the scope of the Government's authority under § 702, and violates Article III and the First and Fourth Amendments to the Constitution. *See* Am. Compl. ¶¶ 165-68. Plaintiffs alleged that the NSA conducts this surveillance "by connecting surveillance devices to multiple major [I]nternet cables, switches, and routers on the [I]nternet backbone," the international submarine and high-capacity terrestrial cables "that carry [I]nternet communications into and out of the United States," *id.* ¶¶ 46, 47, 60. They described the collection as a four-stage process: (1) copying, during which the NSA allegedly "makes a copy of substantially all international text-based communications" "flowing across certain high-capacity cables, switches, and routers"; (2) filtering, during which "[t]he NSA attempts to filter out and

[1] Previously, Upstream collection included Internet communications "that were to, from or about (*i.e.*, containing a reference in the communication's text to) a selector tasked for acquisition under Section 702." FISC Mem. Op. & Order, at 16 (April 26, 2017), https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf. As of March 2017, however, the NSA ceased "abouts" collection entirely. *Id.* at 23, 25.

discard some wholly domestic communications from the stream of internet data"; (3) review of the copied communications for targeted selectors; and (4) retention of "all communications that contain selectors associated with its targets, as well as those that happened to be bundled with them in transit," which "NSA analysts may read, query, data-mine, and analyze." *Id.* ¶ 49.

Plaintiffs alleged that their communications have been and will be subjected to Upstream copying and review based on two theories. First, they alleged that the NSA "intercept[s], cop[ies], and review[s] substantially *all* international text-based communications"—including theirs—"as they transit [U.S.] telecommunications networks." *Id.* ¶ 56 (emphasis added). Second, they alleged it is "virtually certain" that the NSA intercepts at least some of their communications because: (i) due to their global distribution, Plaintiffs' communications "almost certainly traverse every international backbone link connecting the United States with the rest of the world"; (ii) the NSA is "using Upstream surveillance to monitor communications at 'international Internet link[s]' on the Internet backbone"; and (iii) at any given link where the NSA is conducting Upstream surveillance, it "must be" copying and reviewing "all international text-based communications" transiting that link in order to "reliably" obtain communications to or from its intelligence targets. Am. Compl. ¶¶ 60-63.

Proceedings To Date

On Defendants' motion, the Court dismissed the Amended Complaint for lack of subject-matter jurisdiction, concluding that Plaintiffs' allegations were too speculative to support their standing. *See Wikimedia*, 143 F. Supp. 3d at 356-62. On appeal, the Fourth Circuit affirmed in part and vacated in part. *Wikimedia*, 857 F.3d at 217. With regard to Plaintiffs' first theory of standing, which the Court of Appeals referred to as "the Dragnet Allegation," it held that Plaintiffs—including Wikimedia—"d[idn't] assert enough facts about Upstream's operational scope to plausibly allege a dragnet," and thus "ha[d] no Article III standing" under that theory. *See id.* at 213.

With regard to the second theory, on which only Wikimedia relied, *id.* at 202 n.3, the Court of Appeals held that Wikimedia had plausibly alleged that the NSA "must be" intercepting at least

some of its communications, *see id.* at 210-11. The Court of Appeals based this conclusion on three "key" allegations: (1) that, given their great volume and worldwide distribution, Wikimedia's "communications almost certainly traverse every international [Internet] backbone link connecting the United States with the rest of the world"; (2) that, due to alleged "*technical rules of how the Internet works*," the NSA "must be copying and reviewing all the international text-based communications that travel across a given link" it monitors if it is to "reliably" conduct Upstream surveillance; and (3) that the NSA is conducting surveillance on "at least one" Internet backbone link. *Id.* at 203, 210-11 (emphasis added). The Court of Appeals held that, at the pleading stage, these allegations were entitled to a presumption of truth, and together made it sufficiently plausible that the NSA is intercepting, copying, and reviewing at least some of Wikimedia's communications. *Id.* at 211.

On remand, this Court authorized jurisdictional discovery. ECF Nos. 117, 123. Both sides served requests for written discovery and production of documents, and took depositions. Defendants objected to many of Plaintiff's discovery requests and deposition questions on grounds, *inter alia*, that responses would reveal classified information protected by the state secrets and related statutory privileges. Plaintiff moved to compel documents and information that the Government had refused to provide on these grounds. Pls.' Mot. to Compel, ECF No. 125-2, at 3-11.

In response, the DNI formally asserted the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1), over the information sought. *See* DNI Decl. In an *in camera, ex parte* declaration, the Deputy Director of the NSA explained in classified detail the basis for the DNI's assertions of privilege, and asserted the NSA's privilege under 50 U.S.C. § 3605(a). *See* Classif. Decl. of George C. Barnes, Dep. Dir., NSA (public version) ("Classif. NSA Decl."), ECF. No. 141-1.[2]

[2] The DNI's and the NSA's assertions of privilege encompassed seven categories of information: (A) individuals or entities subject to Upstream surveillance; (B) operational details of the Upstream collection process such as the technical details concerning methods, processes, and devices employed (including the design, operation, and capabilities of the devices); (C) locations (and nature of the locations) at which Upstream surveillance is conducted; (D) the specific types or

The Court held that Defendants had satisfied the requirements for asserting the state secrets privilege over the information Plaintiff sought. *See Wikimedia*, 2018 WL 3973016, at *12-14. The Court noted that Defendants had provided "detailed descriptions" explaining why disclosure of this information created a "reasonable, and indeed likely, danger" of "expos[ing] matters which should not be divulged in the interest of national security." *Id.* at 12. So concluding, the Court denied Plaintiff's motion to compel, because the information it sought "falls squarely within the ambit of the state secrets privilege." *Id.* The legal import of that ruling is clear: "a court's determination that a piece of evidence is a privileged state secret removes it from the proceedings entirely." *Abilt v. CIA*, 848 F.3d 305, 313 (4th Cir. 2017).

STATEMENT OF UNDISPUTED MATERIAL FACTS

Because Plaintiff's Dragnet Allegation fails as a matter of law, as held by the Fourth Circuit, the only material facts are those that pertain to Plaintiff's allegation that the NSA, as a technical matter, "must be" copying, and reviewing at least some of its online communications in the course of conducting Upstream surveillance. As discussed in detail below, Defendants are entitled to judgment on this allegation, as well, for three reasons: (i) Plaintiff has adduced no evidence that Upstream surveillance is actually conducted at any "international backbone link" on which its communications supposedly transit; (ii) Plaintiff has adduced no evidence that the NSA, as a technical matter, "must be" copying and reviewing all communications, including Plaintiff's, at any link it monitors; and (iii) undisputed expert testimony demonstrates that this allegation is in fact wrong. The undisputed material facts as to each of these grounds are set out separately below.

---

categories of communications either subject to or acquired in the course of the Upstream collection process; (E) the scope and scale on which Upstream collection has or is now being conducted; (F) the NSA's cryptanalytic capabilities or limitations; and (G) additional categories of classified information encompassed within numerous FISC opinions and orders. *See* DNI Decl. ¶¶ 18, 21-47; Classif. NSA Decl. ¶¶ 54-129.

Plaintiff Has Adduced No Evidence of the Location(s) at Which Upstream Surveillance is Conducted

1. One of the three key allegations on which Plaintiff's standing theory is based is the allegation that the NSA conducts Upstream surveillance on at least one international backbone link transited by Wikimedia's communications. Am. Compl. ¶¶ 60, 61; *Wikimedia*, 857 F.3d at 204-05.

2. This Court upheld the Government's assertion of the state secrets privilege over information concerning "locations at which Upstream surveillance is conducted," *Wikimedia*, 2018 WL 3973016, at *12, 14, including the nature of those locations, *see* DNI Decl. ¶ 18(C), and therefore denied Plaintiff's motion to compel disclosure of such information.

3. Plaintiff has adduced no admissible evidence of its own concerning the nature of the locations at which the NSA currently conducts Upstream surveillance, or otherwise to support its allegation that Upstream surveillance is conducted at "international backbone link[s]," Am. Compl. ¶ 61, allegedly transited by Wikimedia's communications.

Plaintiff Has Adduced No Evidence That, as a Matter of Technological Necessity, the NSA "Must Be" Copying and Reviewing All International, Text-Based Communications that Travel Across Any Given Link at Which Upstream Surveillance Is Conducted

4. A second key allegation on which Plaintiff's standing claim is based is the assertion that the NSA, "for technical reasons . . . must be copying and reviewing all the international text-based communications that travel across a given link upon which [the NSA] has installed [Upstream] surveillance equipment" in order "to reliably obtain communications to [or] from . . . its targets." *Wikimedia*, 857 F.3d at 210; Am. Compl. ¶¶ 62-63.

5. The record contains no admissible evidence to support this allegation.

Undisputed Expert Testimony Shows That There Are Technically Feasible, Readily Implemented Means by Which Upstream Surveillance Could Be Conducted Without Intercepting, Copying, or Reviewing Wikimedia's Communications

6. In addition, expert testimony in the record rebuts Plaintiff's allegation that the NSA, as a matter of technical necessity, "must be" copying and reviewing all the international text-based

communications that cross any given link where Upstream surveillance is conducted. Defs.' Exh. 1, Declaration of Dr. Henning Schulzrinne (filed herewith) ("Schulzrinne Decl.").

7. There are a number of technically feasible, readily implemented means by which the NSA could be conducting Upstream surveillance without intercepting, copying, or reviewing all communications transiting any Internet backbone link at which the NSA might hypothetically be conducting Upstream collection. Schulzrinne Decl ¶¶ 15, 53, 77.

8. These methods could readily be employed to conduct Upstream surveillance without intercepting, copying, or reviewing, specifically, Wikimedia's communications, regardless of the number or nature of the location(s) at which Upstream surveillance is conducted. *Id.* ¶ 90.

9. The Internet is a global collection of large and small networks that function as a single, large virtual network, on which any device connected to the network can communicate with any other connected device. *Id.* ¶ 16.

10. To communicate over the Internet an individual user connects with the network of a local Internet Service Provider ("ISP"), either directly (typically for a monthly fee) or indirectly through an organization (*e.g.*, a place of business). In turn, the local ISP's network connects, at locations known as points of presence ("POPs"), to the networks of still larger regional and national ISPs, the largest of which are so-called "Tier 1" telecommunication service providers. *Id.* ¶¶ 17-18.

11. Tier 1 providers and other large carriers maintain high-capacity terrestrial fiber-optic networks, known generally as Internet "backbone" networks, that use long-haul terrestrial cables to link large metropolitan areas across entire nations or regions. Data travel across these cables in the form of optical signals, or pulses of light. Tier 1 providers and other large carriers typically interconnect their networks using high-capacity routers either directly, at facilities known as peering stations, or through public Internet exchange points ("IXPs"), to make possible communications between users of different providers' networks. *Id.* ¶¶ 19-20. Tier 1 providers and other large

carriers typically connect separate legs of their own networks at facilities known as points of presence ("POPSs"), using high-capacity switches. *Id.* ¶¶ 17-19.

12. The Internet backbone also includes transoceanic cables linking North and South America with each other and with Europe, Asia, the Middle East, and Africa. These undersea cables reach shore at points known as cable landing stations, from which they are linked to nearby Internet exchange points and the terrestrial telecommunications network. *Id.* ¶¶ 21-23.

13. Generally speaking, to send a communication on the Internet, the transmitting device (e.g., a personal computer, a cell phone, or the computer—a.k.a. "server"—on which a website is physically stored) first converts the communication into one or more small bundles of data called "packets," configured according to globally accepted protocols. *Id.* ¶¶ 25-26.

14. When a communication is broken into separate packets, each packet includes (i) a "header," that is, the routing, addressing and other technical information required to facilitate the packets' travel from their source to their intended destination, and (ii) a "payload," that is, a portion of the contents of the communication being transmitted. *Id.* ¶ 28.

15. A packet's header contains three relevant pieces of address and routing information: (i) the packet's source and destination Internet Protocol ("IP") addresses; (ii) the source and destination port; and (iii) protocol numbers. *Id.* ¶ 29.

16. IP Addresses: IP addresses are unique numeric identifiers assigned to particular computers, devices, or systems connected to the Internet, which are used to direct data sent from one computer or other online device to one or more other devices, and back. IP addresses may be analogized to the destination and return addresses on a mailing envelope. *Id.* ¶ 30.

17. Each Internet Service Provider or other large enterprise with a fixed presence on the Internet, including Wikimedia, acquires blocks of "static" IP addresses assigned on a permanent basis from the appropriate regional Internet registry affiliated with global Internet Assigned

Numbers Authority ("IANA"). *Id.* ¶¶ 32-33. There are public databases that record, with very high accuracy, which address blocks are used by what entities. *Id.* ¶ 32.

18. Ports: Ports are numbers also included in packet headers, used to identify communications of different kinds (*e.g.*, webpage requests, or email) so that servers hosting multiple communications services (*e.g.*, a website, an email service) can distinguish packets destined for one service from those meant for another. Users' devices (home computers, cellphones) that run multiple applications (*e.g.*, web browsing, email) similarly rely on port numbers contained in packet headers to ensure that packets of each given type are routed to the appropriate applications on their personal devices. *Id.* ¶ 35. While IP addresses can be analogized to the street address on a letter, port numbers are roughly analogous to the apartment numbers at a multi-unit dwelling. *Id.* ¶ 36.

19. Port numbers for common applications like web-browsing and email, are assigned in a common industry registry maintained by the IANA. *Id.*

20. Protocol Numbers: Protocols associated with various layers of the network architecture are also assigned numbers maintained in a registry by the IANA. Protocol numbers are also included in packet headers and used by receiving devices to determine the appropriate protocols to apply for interpreting and acting on each packet upon arrival. *Id.* ¶ 38.

21. Once a communication has been broken into packets by the transmitting device, specialized computers called routers and switches ensure that the packets travel an appropriate path across the Internet to their destination IP address. High-capacity carrier-grade routers are located at peering stations, IXPs, and POPs, routing packets from one network to another. Carrier-grade switches are typically located at POPs, where different legs of the same carrier backbone network interconnect, and forward packets from one leg of the network to another. *Id.* ¶ 39.

22. Each router or switch through which a packet transits on its path scans the packet's header information, including its destination IP address, and using an internal routing table, and performance-based rules that account for network congestion and outages, determines which

direction (path) the packet should follow next in order to reach its intended destination. The largest routers and switches handle millions of data packets every second. *Id.* ¶ 40.

23. To protect the privacy and integrity of information, users sending data across the Internet may choose to encrypt their traffic, *i.e.*, encode the data mathematically, so that it can only be read by parties who have the encryption key. The most common encryption mechanism is the HTTP-over-TLS protocol, also referred to as the HTTPS protocol, used to encrypt web communications. Despite its relation to the HTTP protocol (used for communications on the World Wide Web), the HTTPS protocol has been assigned a different port, port 443, whereas the unencrypted HTTP protocol is assigned port 80. *Id.* ¶ 42.

24. When the packets making a communication arrive at the receiving computer, smartphone, or other device, the operating system of the receiving device reassembles the packets into the original communication, such as a webpage or email. *Id.* ¶ 44.

25. Wikimedia is incorrect that the NSA, at any given link where Upstream collection is conducted, must, as a matter of technical necessity, be intercepting, copying, and reviewing all communications crossing that link (including, therefore, Wikimedia's). There are a number of technically feasible, readily implemented means of conducting Upstream-type surveillance that would not require intercepting, copying, or reviewing communications that traverse any Internet backbone link the NSA allegedly monitors. *Id.* ¶ 53.

26. These methods involve selectively copying only those communications that are deemed more likely to include communications of interest, using routers and switches to "mirror" selected communications carried in a given stream of communications traffic. *Id.* ¶ 57.

27. Traffic "mirroring" is a process by which a router or switch, in addition to determining where on the Internet each packet should be forwarded next, can also identify certain packets to be copied ("mirrored") and divert the designated copies off-network for separate processing. *Id.* ¶ 58.

28. Traffic mirroring is accomplished by programming routers and switches with so-called access control lists ("ACLs") to determine whether packets will be forwarded or blocked at a given interface, that is, a given link between the router or switch and another device. The criteria used in the ACL associated with each interface can include a packet's source or destination IP address, the port number, protocol numbers, or other information contained in a packet header. *Id.* ¶¶ 60-61.

29. The router or switch examines the header information of each packet it processes, and compares it to the ACL for each interface, to determine which interfaces the packet may or may not pass through. At each interface whose ACL criteria the packet satisfies, the router or switch then creates a separate copy of the packet, and allows it to pass through that interface. *Id.*

30. Tier 1 and other providers employ traffic mirroring in the normal course of operations for such purposes as monitoring traffic load, conducting quality-control processes, and rejecting unwanted traffic (*e.g.*, traffic from suspicious sources). *Id.* ¶ 58.

31. At any given link on the Internet where surveillance may be conducted, traffic mirroring with ACLs could be used in several ways to make only certain packets available for inspection by a collecting entity. *Id.* ¶ 64.

32. Initially, it would be necessary to establish an interface (a fiber-optic link) between the router or switch directing traffic at that location, and the separate equipment used by the collecting entity (hereinafter, the "collector interface"). *Id.*

33. Once the link is established, traffic passing through the carrier's router, or switch, to the collector's equipment could be filtered by "whitelisting" or "blacklisting" techniques that involve configuring an ACL to allow only packets meeting the ACL's criteria to be copied and passed through the collector interface to the collector's equipment. *Id.* ¶¶ 65, 67.

34. For example, if the collecting entity possesses information that communications of interest are associated with particular IP addresses, the carrier could configure an ACL for the collector interface containing a "whitelist" of the specified IP addresses. When the router or switch

examines the header information of each packet it processes, it would then, (i) as usual, forward a copy of the packet toward its intended destination, (ii) perhaps forward additional copies through other interfaces, per the carrier's routine business practices, and (iii) if, but only if, the packet header contains a source or destination IP address on the whitelist, create an additional copy of the packet, and forward it through the collector interface into the collector's possession and control. *Id.* ¶ 65.

35. Packets not meeting the whitelist criteria would not be copied for, or made available to, the collector's equipment for any purpose, and would not be handled or processed in any way other than would ordinarily occur under the carrier's routine practices. *Id.* ¶ 66.

36. Blacklisting, conversely, involves configuring an access control list to allow all packets to pass through the collector interface *except* those matching the ACL's criteria. If the collecting entity concludes that communications to and from certain IP addresses are of little interest, then the carrier could configure the ACL for the collector interface with a "blacklist" of the specified IP addresses. The router or switch would then, as usual, examine each packet header and (i) forward each packet toward its destination on the Internet, (ii) create packet copies and forward them through interfaces specified by the carrier's business practices, and (iii) create an additional copy of each packet, and forward it through the collector interface into the collector's possession and control, except for those packets with source or destination IP addresses on the blacklist. *Id.* ¶ 67.

37. If on examination a packet header is found to contain a source or destination IP address on the blacklist, an additional copy of that packet is not created or forwarded through the collector interface into the possession and control of the collecting entity, and is not handled or processed in any way other than would ordinarily occur under the carrier's routine practices. *Id.* ¶ 67.

38. Whitelisting and blacklisting techniques can also be used to limit mirroring to particular sources of traffic, such as communications from cables used by specific carriers, or cables linked to specific countries or regions. *Id.* ¶ 69.

39. In addition, ACLs can be configured to whitelist or blacklist particular types of communications, with different protocols, based on their port or protocol numbers. For example, if the collecting entity is interested only in email, the carrier could configure the ACL for the collector interface to create additional copies of packets, and forward them into the collector's possession and control, only if the port number contained in the packets' headers is either port 25 or port 143 (the default ports for the two email protocols, "SMTP" and "IMAP"). If conversely the collecting entity does not wish access to web communications encrypted with the HTTPS protocol (perhaps because it cannot decipher them), then the carrier could configure an ACL for the collector interface that allows no packets containing port number 443 (the default port for HTTPS communications) to be copied and passed into the collecting entity's possession and control. *Id.* ¶¶ 36, 70.

40. Wikimedia posits a highly similar scenario in its Amended Complaint, in which video traffic of allegedly no interest to the NSA is "ignore[d]." Am. Compl. ¶ 59. To achieve that result, a carrier could configure the ACL for the interface with the NSA's surveillance equipment to block any packets whose source IP addresses correspond to streaming video services whose traffic the NSA did not wish to examine. Schulzrinne Decl. ¶ 72.

41. Because of the availability of these traffic-mirroring techniques, it is not the case, as Plaintiff alleges, Am. Compl. ¶ 62, that the NSA must copy and review all international, text-based communications traversing a link in order to "reliably" identify those of interest. For example, if a collecting entity were sufficiently confident that the communications of interest to it are associated with particular IP addresses, or, conversely, that communications to and from certain IP addresses do not include communications of interest, then by whitelisting or blacklisting communications to and from those high- or low-interest IP addresses, respectively, it could reliably obtain all communications of interest that are crossing that link, without copying and reviewing all of the communications traversing the link. Schulzrinne Decl. ¶ 73.

42. In light of available traffic-mirroring techniques, it is also not so, as Plaintiff alleges, Am. Compl. ¶ 63, that the NSA must copy and review all communications traversing a link in order to reassemble communications and review them for targeted selectors. For example, all packets in a communication to or from a target will have a common destination or source IP address, respectively. If the collecting entity obtains access to all packets crossing the link containing that address, it will have all the packets making up that communication, and can reconstruct it. If confident it has identified the IP addresses of high- or low-interest communications, then through whitelisting or blacklisting the collecting entity can obtain (and reassemble) all packets constituting those communications without copying all packets crossing the link. Schulzrinne Decl. ¶¶ 75-76.

43. Wikimedia has identified three categories of its communications that it contends are subjected to Upstream collection processes: (Category 1) communications with and among its "community members" who read or contribute to its Projects and webpages, or use the Projects and webpages to interact with each other; (Category 2) its internal log communications; and (Category 3) electronic communications of its staff. Defs.' Exh. 3, Pl.'s Am. & Supp. Resps. & Objs. to NSA's 1st Set of Interrogatories, No. 3. Using the traffic-mirroring techniques discussed above, the communications in all three of these categories could readily be blocked from alleged NSA surveillance equipment. Schulzrinne Decl. ¶¶ 77-88; *see* Am. Compl. ¶ 47.

44. Category 1: According to Wikimedia, the first category, communications with and among Wikimedia's community members, consists of requests from foreign and domestic users to view or download content from Wikimedia websites, using the HTTP and HTTPS protocols, and email communications sent from foreign users to Wikimedia servers, using the SMTP protocol, all destined for Wikimedia IP addresses. Defs.' Exh. 4, Pl.'s Am. Resps. & Objs. to ODNI Interrog. No. 19, Ex. 1 (hereinafter, "Technical Statistics Chart").

45. According to Wikimedia, the volume of the SMTP email communications in the first category, and the countries from which they are received, are unknown. Technical Statistics Chart.

46. At any Internet backbone link where Upstream surveillance might hypothetically be conducted, NSA access to all HTTP and HTTPS communications crossing that link, including Wikimedia's, could be blocked by "blacklisting" all packets with port numbers 80 and 443, respectively, so that none are copied, forwarded to alleged NSA surveillance equipment, or otherwise passed into NSA possession or control. Schulzrinne Decl. ¶ 79; *see* Am. Compl. ¶ 47.

47. At any Internet backbone link where Upstream surveillance might hypothetically be conducted, NSA access to communications crossing that link that contain source or destination IP addresses used by Wikimedia, including all Category 1 HTTP, HTTPS, and SMTP communications, could be blocked by "whitelisting" or "blacklisting" by IP address, so that no communications to or from Wikimedia would be copied, forwarded to alleged NSA surveillance equipment, or otherwise passed into NSA's possession or control. Schulzrinne Decl. ¶¶ 80-82; *see* Am. Compl. ¶ 47.

48. Category 2: According to Wikimedia, the second category of communications on which it relies to establish its standing are "internal log communications," transmitted from its servers in the Netherlands to its servers in the United States. These communications are encrypted using a protocol known as IPSec, using one of the same Wikimedia IP addresses as Wikimedia's Category 1 communications. Technical Statistics Chart; Schulzrinne Decl. ¶ 83.

49. At any link where Upstream surveillance might hypothetically be conducted, NSA access to Wikimedia's server log communications transiting that link could be blocked in one of two ways. First, all communications crossing that link encrypted with the IPSec protocol, including Wikimedia's, could be blocked by "blacklisting" all packets with protocol number 50 (the protocol number assigned to the IPSec protocol). Second, NSA access to Wikimedia's log communications, like its Category 1 communications, could be blocked by whitelisting or blacklisting by IP address. In either case, none of Wikimedia's log communications transiting the link would be copied, forwarded to alleged NSA surveillance equipment, or otherwise passed into NSA's possession or control. Technical Statistics Chart; Schulzrinne Decl. ¶ 84; *see* Am. Compl. ¶ 47.

50. Category 3: The third category of communications on which Wikimedia relies to establish its standing are international communications by Wikimedia's staff, using various protocols, some of which communications are encrypted, and some not. These communications, like those in Categories 1 and 2, are sent and received from IP addresses assigned to and used by Wikimedia. At any Internet backbone link where Upstream surveillance might hypothetically be conducted, NSA's access to any of Wikimedia's staff communications transiting that link could be blocked by whitelisting or blacklisting by IP address, so that none of Wikimedia's staff communications transiting the link would be copied, forwarded to NSA's surveillance equipment, or otherwise passed into NSA's possession or control. Technical Statistics Chart; Schulzrinne Decl. ¶¶ 85-87.

51. At any given Internet backbone link, the NSA could conduct Upstream surveillance in a manner such as Wikimedia alleges without intercepting, copying, or reviewing Wikimedia's communications. Therefore, the NSA could do so regardless of the number of such links at which Upstream surveillance might be conducted. Schulzrinne Decl. ¶ 90.

ARGUMENT

I. LEGAL STANDARDS

A. Summary Judgment Standard

Summary judgment should be granted if there is no "no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). A fact is material if it "might affect the outcome of the suit," and a dispute is genuine if "the evidence is such that a reasonable [trier of fact] could" rule in favor of the nonmoving party on that issue. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). "[T]here can be no genuine issue as to any material fact," however, where a party "fails to make a showing sufficient to establish the existence of an element essential to that party's case, and on which [it] [bears] . . . the burden of proof." *Celotex Corp. v. Catrett*, 477 U.S. 317, 322-23 (1986).

Because a demonstration of standing is an "indispensable part of [Plaintiff's] case," Wikimedia must support its standing "in the same way as any other matter on which [it] bears the burden of proof, *i.e.*, with the manner and degree of evidence required at [each] successive stage[ ] of the litigation." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992). Thus, if Plaintiff cannot set forth, by affidavit or other evidence that will be in admissible form at trial, "specific facts" sufficient to show a genuine issue for trial on standing, then "Rule 56(c) mandates the entry of summary judgment" against it. *Celotex*, 477 U.S. at 322 & n.3 (quoting Fed. R. Civ. P. 56(e)).

B. The Requirements of Standing

"Article III of the Constitution limits federal courts' jurisdiction to certain 'Cases' and 'Controversies.'" *Amnesty Int'l*, 568 U.S. at 408. "[N]o principle is more fundamental to the judiciary's proper role" under the Constitution's separation of powers. *Id.*; *see also Spokeo, Inc. v. Robins,* 136 S. Ct. 1540, 1547 (2016). "[A]n essential and unchanging part of the case-or-controversy requirement" is that litigants have "standing to invoke the authority of a federal court," *DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 342 (2006), assuring that would-be litigants have a sufficient "personal stake in the outcome of [a] controversy as to . . . justify [the] exercise of the court's remedial powers on [their] behalf." *Town of Chester v. Laroe Estates, Inc.*, 137 S. Ct. 1645, 1650 (2017). Standing is, therefore, a "threshold jurisdictional question," *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 102 (1998), "determining the power of the court to entertain the suit," *Warth v. Seldin*, 422 U.S. 490, 498 (1975). The standing inquiry must be "especially rigorous when reaching the merits of the dispute would force [a court] to decide whether an action taken by one of the other two branches of the Federal Government," particularly "in the fields of intelligence gathering and foreign affairs," "was unconstitutional." *Amnesty Int'l*, 568 U.S. at 408-09.

To establish Article III standing, Plaintiff must seek relief from an injury that is "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling." *Id.* at 409. To show injury in fact, "a plaintiff must show … an invasion of a

legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical." *Wikimedia*, 857 F.3d at 207. Speculative claims of injury will not support Article III standing. *See Amnesty Int'l*, 568 U.S. at 413-14; *Wikimedia*, 857 F.3d at 208. And where, as here, a plaintiff seeks prospective declaratory and injunctive relief to prevent a threatened injury, *see* Am. Compl. at 55 (Prayer for Relief ¶¶ 2-4), the "threatened injury must be *certainly impending* to constitute injury in fact." *Amnesty Int'l*, 568 U.S. at 409-10.

II. DEFENDANTS ARE ENTITLED TO SUMMARY JUDGMENT, BECAUSE PLAINTIFF HAS NOT ESTABLISHED ITS STANDING TO SUE.

A. Reliance on Plaintiff's "Dragnet Allegation" Is Foreclosed by the Court of Appeals' Decision.

Previously Plaintiff advanced a theory of standing based on the alleged scope of Upstream collection, arguing that its communications must be among those the NSA copies and reviews because, according to Plaintiff, Upstream surveillance involves "intercepting, copying, and reviewing substantially *all* international text-based communications." Am. Compl. ¶ 56 (emphasis added). The Fourth Circuit termed this the "Dragnet Allegation," *see Wikimedia*, 857 F.3d at 202, and held that it "fails to establish standing" because it "lacks sufficient factual support to get 'across the line from conceivable to plausible,'" *id.* at 213-14 (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). Despite that binding determination that the Dragnet Allegation cannot support standing as it is currently pled, Plaintiff states that it may still rely on this theory to attempt to establish the Court's jurisdiction. *See* Defs.' Exh. 5, Pl.'s Resps. & Objs. to NSA's 1st Set of Interrogs., No. 1. Under the well-established "mandate rule," the Fourth Circuit's decision forecloses any such effort.

"[F]ew legal precepts are as firmly established as the doctrine that the mandate of a higher court is controlling as to matters within its compass." *Invention Submission Corp. v. Dudas*, 413 F.3d 411, 414 (4th Cir. 2005) (quotation omitted). "The mandate rule governs what issues the lower court is permitted to consider on remand—it is bound to carry out the mandate of the higher court, [and] may not reconsider issues the mandate laid to rest." *United States v. Susi*, 674 F.3d 278, 283 (4th

Cir. 2012). "Deviation from the mandate rule is permitted only in a few exceptional circumstances," which are not present here. *See Invention Submission Corp.*, 413 F.3d at 415.

The Fourth Circuit unequivocally rejected Plaintiff's Dragnet Allegation as insufficient, as a matter of law, to establish Plaintiff's standing. Now that the Fourth Circuit has laid the allegation to rest, Plaintiff is not at liberty to disinter it.

B. Plaintiff Has Presented No Admissible Evidence To Support Its Allegation That Upstream Surveillance Is Conducted at "International Internet Links" That Its Communications Allegedly Traverse.

Plaintiff's remaining theory of standing depends on three facts making it "virtually certain," in Plaintiff's view, that the NSA intercepts at least some of its communications. Am. Compl. ¶ 60. As alleged by Plaintiff, and held by the Fourth Circuit, this theory depends on proof that: (i) due to their global distribution, Wikimedia's communications "almost certainly traverse every international backbone link connecting the United States with the rest of the world"; (ii) that the NSA is "using Upstream surveillance to monitor communications at 'international Internet link[s]' on the Internet backbone"; and (iii) that at any given link where the NSA is conducting Upstream surveillance, it "must be" copying and reviewing "all international text-based communications" transiting that link in order to "reliably" obtain communications to or from its intelligence targets. Am. Compl. ¶¶ 60-63; *see also Wikimedia*, 857 F.3d at 209-211. But when removed from the realm of theory and put to the test of proof, this argument also fails, because Plaintiff lacks admissible evidence sufficient to establish two of the three "key" facts on which the argument vitally depends. *Id.* at 210-11.

The first of these unsubstantiated allegations is Plaintiff's assertion that the NSA conducts Upstream surveillance on at least one international Internet backbone link transited by Wikimedia's communications. Am. Compl. ¶ 60; *Wikimedia*, 857 F.3d at 203-04, 211. The Court could assume *arguendo* that Plaintiff has presented sufficient evidence to support a conclusion that its communications "almost certainly traverse every international backbone link connecting the United States to the rest of the world." Am. Compl. ¶ 61. But without evidence that the NSA actually

conducts Upstream surveillance at one or more of these "international backbone links," there is no basis in the record to conclude that the NSA actually monitors any link transited by Wikimedia's communications. Without such evidence, Wikimedia cannot show that its communications have been or will be intercepted, copied, or reviewed by the NSA in the course of Upstream surveillance.

To be sure, Plaintiff sought evidence in discovery to support this allegation, and moved to compel disclosures of information about the locations where Upstream surveillance is conducted. In particular, Plaintiff sought to compel interrogatory responses, admissions, and the production of documents it believed would prove that Upstream collection is conducted on one or more international Internet links. *See* Pl's. Mot. to Compel, at 5, 7. But the DNI asserted the state secrets privilege over information concerning the locations at which Upstream surveillance is conducted, including the nature of those locations. DNI Decl. ¶ 18(C). The Court rightly upheld the Government's claim of privilege over this information, and denied Plaintiff's motion to compel. *Wikimedia*, 2018 WL 3973016, at *10-14. As a result, any evidence concerning the nature or location of sites where Upstream surveillance is conducted "is remove[d] from the[se] proceedings entirely." *El-Masri v. United States*, 479 F.3d 296, 306 (4th Cir. 2007); *Abilt*, 848 F.3d at 313.

Without evidence that the NSA conducts Upstream collection on at least one international backbone link, Plaintiff cannot establish one of the three "key" facts necessary to show its standing. *See Wikimedia*, 857 F.3d at 210-11. And without such proof, Plaintiff is left with "a complete failure of proof concerning an essential element of [its] case." *Celotex*, 477 U.S. at 323; *Defenders of Wildlife*, 504 U.S. at 561. On this basis alone, Rule 56 mandates entry of judgment for the Government. *Celotex*, 477 U.S. at 322-23; *Williams v. Genex Servs., LLC*, 809 F.3d 103, 109 (4th Cir. 2015).

C. Plaintiff Has Presented No Admissible Evidence for Its Allegation That the NSA "Must Be" Intercepting, Copying, and Reviewing All International Text-Based Communications Traversing a Given Internet Backbone Link.

The second pivotal allegation on which Plaintiff's remaining theory of standing depends is the assertion that the NSA, "for technical reasons . . . must be copying and reviewing all the

international text-based communications that travel across a given link" monitored by the NSA, in order "to reliably obtain communications to [or] from . . . its targets." *Wikimedia*, 857 F.3d at 210-11; *see* Am. Compl. ¶ 62. Proof of this allegation is essential to Plaintiff's standing argument, as the Court of Appeals recognized, *Wikimedia*, 857 F.3d at 210-11, in order to show, even if the NSA were monitoring a link transited by Wikimedia's communications, that Wikimedia's communications would in fact be among those intercepted, copied, and reviewed by the NSA at that link. This is also an allegation, however, for which Plaintiff has yet to offer any evidence.

Once again, Plaintiff sought to elicit information in discovery that it believed would support this allegation. *See* Pl.'s. Mot. to Compel at 3. But again the DNI asserted a claim of privilege, which the Court properly sustained, over the information Plaintiff sought. *See* DNI Decl. ¶ 18(B), (D) (asserting privilege over operational details of the Upstream collection process, including "the design, operation, and capabilities of the devices," and "the specific types or categories of communications either subject to or acquired in the course of [the] process"); *Wikimedia*, 2018 WL 3973016, at *10-14. The result again is that the information Plaintiff sought "is remove[d] from the proceedings entirely," *El-Masri*, 479 F.3d at 306; *Abilt*, 848 F.3d at 313, and Plaintiff is left with "a complete failure of proof concerning an essential element of [its] case." *Celotex*, 477 U.S. at 323; *Defenders of Wildlife*, 504 U.S. at 561. For this reason, too, judgment must be entered for Defendants as a matter of law. *Celotex*, 477 U.S. at 322-23; *Williams*, 809 F.3d at 109.

D. In Addition, Undisputed Expert Testimony Rebuts Plaintiff's Allegation That, as a Technical Matter, the NSA "Must Be" Intercepting, Copying, and Reviewing at Least Some of Wikimedia's Communications.

Defendants are entitled to summary judgment for yet a third reason. Not only has Plaintiff failed to adduce evidence to support its key allegation that the NSA "must be" copying and reviewing all communications transiting any Internet backbone link where Upstream collection is conducted; undisputed expert testimony shows that, as a technical matter, Plaintiff's allegation is wrong. In the words of computer science expert (and Columbia University Professor) Dr. Henning

Schulzrinne,[3] "there are a number of technically feasible, readily implemented means of conducting Upstream surveillance that would not require interception, copying, or reviewing all communications that traverse any Internet backbone link the NSA allegedly monitors." Schulzrinne Decl. ¶ 53.

Therefore, "Wikimedia's assertion that the NSA, in the course of conducting Upstream surveillance, must, as a matter of technological necessity, be intercepting, copying, and reviewing at least some of Wikimedia's electronic communications that traverse any Internet backbone 'link' monitored by the NSA" is also "incorrect." *Id.* ¶ 15. *See also id.* ¶¶ 1, 51, 53, 85. Dr. Schulzrinne's conclusion, is firmly rooted in "the technical rules of how the Internet works," *Wikimedia*, 857 F.3d at 210, and he explains why those rules do not, in fact, "require" that the NSA conduct Upstream surveillance in the manner that Wikimedia alleges. *See id.* at 210-11.[4]

If Upstream collection occurs, as Wikimedia alleges, at Internet backbone "links" such as Internet exchanges or points of presence, with the assistance of telecommunications service providers, *see* Am. Compl. ¶¶ 47-49, then for purposes of surveillance the routers and switches that direct the flow of communications traffic at these locations could be used to implement selective, rather than wholesale, copying and scanning of communications links through "traffic mirroring," *see* Statement of Material Facts ("St. Mat. Fact"), *supra* ¶¶ 27-42. A routine business practice conducted by carriers, traffic mirroring involves programming routers and switches with access

[3] Dr. Schulzrinne is the Julian Clarence Levi Professor of Computer Science at Columbia University, where he has been a faculty member since 1996. From 2012 to 2017, he was also Chief Technology Officer of the Federal Communications Commission, where he guided FCC policy on technology and engineering issues. He received his PhD in Electrical Engineering from the University of Massachusetts at Amherst in 1992. Dr. Schulzrinne also heads Columbia's Real-Time Internet Laboratory, which under his supervision conducts research in the areas of real-time Internet multimedia services and Internet telephony, among others. Over the course of his career, Dr. Schulzrinne has co-developed a number of Internet protocols, and published more than 250 journal and conference papers in his field. Among his many professional associations, honors, and awards, in 2006 he was named a Fellow of the Institute of Electrical and Electronics Engineers (IEEE), in recognition of his many contributions to the design of protocols and applications for Internet multimedia. He was inducted into the Internet Hall of Fame in 2013. *See* Schulzrinne Decl. ¶¶ 3-12.

[4] In reaching his conclusions, Dr. Schulzrinne has not considered or been provided with any classified or other non-public information about Upstream collection. Schulzrinne Decl. ¶¶ 14, 49.

control lists that use criteria as communications' source or destination IP addresses, ports, or protocol numbers to determine whether copies of individual communications will be blocked or forwarded at a given interface, or link, between a router or switch and other devices to which the router or switch is connected. *Id.* ¶¶ 27-30.

At any given backbone link where surveillance may be conducted, traffic mirroring designed to make only certain communications available for inspection by a collecting entity could be accomplished using either a "whitelisting" or a "blacklisting" approach. *Id.* ¶¶ 31-33. For example, if a collecting entity determines that communications of interest to it are associated with particular IP addresses, then the carrier at that location could configure an access control list with a "whitelist" of these addresses. When the router or switch examines the header of each packet it processes, it would, as usual, forward the packet toward its intended destination, but if (and only if) the packet header also contained a source or destination IP address on the whitelist, then the router or switch would create an additional copy of the packet and forward it through the interface with the collecting entity's equipment (the collector interface) into the collecting entity's possession or control. *Id.* ¶ 34. Conversely, if the collecting entity determined that communications to and from certain IP addresses are of little interest, then the carrier could configure a "blacklist" that would cause its router or switch to create an additional copy of each communications packet it processes and to forward it through the collector interface to the collecting entity's possession and control, *except* for those packets containing source or destination IP addresses on the blacklist. *Id.* ¶ 36.

Under these approaches, if a packet's source or destination IP address does not meet the whitelist criteria, or if it has a source or destination IP address that is included on the blacklist, then an additional copy of the packet is not created, nor forwarded through the collector interface to the collector's possession and control. Indeed, the packet would not be handled or processed in any way other than what would ordinarily occur under the carrier's routine practices. *Id.* ¶¶ 35, 37.

Particular types of communications can also be whitelisted or blacklisted, based on the port or protocol numbers contained in their packet headers. For example, if a collecting entity only wished access to email communications, they could be whitelisted using the port numbers (25 and 143, respectively) associated with email. Conversely, if a collecting entity did not wish access to web communications encrypted with the HTTPS protocol, then they could be blacklisted using port number 443. St. Mat. Fact. ¶¶ 38-39. Wikimedia itself speculates that Upstream is conducted in a manner such that video traffic of allegedly no intelligence interest to the NSA is "ignored," *i.e.* blacklisted, from access to the NSA's surveillance equipment. *Id.* ¶ 40; Am. Compl. ¶ 59.

Because of these available methods for selectively choosing which communications are copied and delivered into the possession and control of a collecting entity at any given Internet backbone link, it is not the case, as Wikimedia alleges, *see* Am. Compl. ¶¶ 62, 63, that the NSA must copy and review all international, text-based communications traversing a link in order to "reliably" identify (or reassemble) those of interest. St. Mat. Fact. ¶¶ 41-42. For example, if a collecting entity were sufficiently confident that the communications of interest to it are associated with particular IP addresses, or, conversely, that communications to and from certain IP addresses do not include communications of interest, then by whitelisting or blacklisting communications to and from those high- or low-interest IP addresses, respectively, it could reliably obtain all packets of all communications of interest that are crossing that link (and reassemble them), without having to copy and review all of the communications traversing the link. *Id.*

It follows readily from this analysis that the NSA could conduct Upstream collection without intercepting, copying, or reviewing any of the categories of Wikimedia's communications allegedly subjected to the Upstream collection process: (1) communications with and among its "community members"; (2) its internal log communications; and (3) electronic communications of its staff. *Id.* ¶¶ 43-44. The first category consists of web communications using the HTTP and HTTPS protocols, and email using the SMTP protocol. The Government has not confirmed whether or not

the NSA collects web communications as part of Upstream surveillance, but if it does not, then it would be a simple matter to block NSA access to all such communications, including Wikimedia's, by blacklisting communications with ports 80 and 443. *Id.* ¶ 46. The SMTP communications in this category, to the extent relevant,[5] could be blocked by whitelisting or blacklisting by IP address (as could the HTTP and HTTPS communications in this category as well). *Id.* ¶ 47.

The second category of Wikimedia's communications, its server log communications, are encrypted using a common protocol known as IPSec, and could be blocked from alleged NSA surveillance equipment, *see* Am. Compl. ¶ 47, at any given link by blacklisting all communications with protocol number 50. Alternatively, NSA access to these communications could be blocked by whitelisting or blacklisting by IP address. *Id.* ¶¶ 48-49. The third and final category of communications on which Wikimedia bases its standing, international communications to and from its staff, could also be blocked through whitelisting or blacklisting by IP address. *Id.* ¶ 50. In all events, none of Wikimedia's communications would be copied, forwarded to alleged NSA surveillance equipment, *see* Am. Compl. ¶ 47, or otherwise passed to NSA possession or control. *See generally* St. Mat. Fact. ¶¶ 46-50. And this would be the case, moreover, regardless of the number of Internet backbone links, if any, at which the NSA conducted Upstream surveillance. *Id.* ¶ 51.

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. Those are facts protected by the state secrets privilege. But what this analysis shows is that there are at least several practical means for conducting Upstream surveillance (at least as Plaintiff conceives it) that would not involve intercepting, copying, or reviewing all communications transiting the links the NSA allegedly monitors. Thus, Dr. Schulzrinne's analysis

[5] Wikimedia acknowledges that it does not know the volume of the SMTP communications in this first category, or the countries from which they are received. St. Mat. Fact ¶ 45. Hence, Wikimedia has made no showing that this sub-category of its communications satisfies even the first criterion, "geographical diversity," *Wikimedia*, 857 F.3d at 210, of its own standing theory.

disproves Plaintiff's hypothesis that NSA interception, copying, or review of all such communications, including Wikimedia's, "must be" occurring. Schulzrinne Decl. ¶ 53.

In other words, this Court's earlier intuition, that regardless of the NSA's capabilities, it need not necessarily be conducting Upstream surveillance "at full throttle," *Wikimedia*, 143 F. Supp. 3d at 356, was prescient. The undisputed evidence rebuts Plaintiff's allegation that the NSA, as a matter of technological necessity, "must be" intercepting, copying, and reviewing all communications, including Wikimedia's, that transit any Internet backbone link the NSA monitors.[6]

III. EVEN IF PLAINTIFF COULD SHOW A GENUINE ISSUE OF MATERIAL FACT, ITS STANDING CANNOT BE LITIGATED WITHOUT EXCLUDED STATE SECRETS, AND UNACCEPTABLE RISK OF DISCLOSING PRIVILEGED INFORMATION.

A fourth reason lies here why judgment must be entered for Defendants. Even assuming that Plaintiff could raise a genuine issue of material fact as to its standing, the standing issue could not be tried without risking or requiring harmful disclosures of privileged state secrets.

In *El-Masri v. Tenet*, this Court recognized that where "circumstances make clear that sensitive military secrets will be so central to the subject matter of the litigation that any attempt to proceed will threaten disclosure of the privileged matters, dismissal is the appropriate remedy.'" 437 F. Supp. 2d 530, 538–39 (E.D. Va. 2006) (quoting *Sterling*, 416 F.3d at 348), *aff'd*, 479 F.3d 296 (4th Cir. 2007). Thus, where the state secrets privilege has been properly invoked, "the question is whether [the plaintiff's] claim could be fairly litigated without disclosure of the state secrets absolutely protected by the United States' privilege." *El-Masri*, 437 F. Supp. 2d at 539. This inquiry encompasses not only whether a plaintiff can make out a *prima facie* case without privileged evidence,

[6] For a variety of reasons, Plaintiff also alleges that there is a "substantial likelihood" that its intercepted communications are also "retained, read, and disseminated" by the NSA. Am. Compl. ¶¶ 71, 104-07. Because Plaintiff cannot show that its communications have been (or will be) intercepted, copied, and scanned, as an initial matter, it necessarily follows that it cannot show that any of its communications have been (or will be) retained, read, and disseminated by the NSA.

but also whether "the main avenues of defense" may be pursued without risk of disclosing privileged information. *Abilt*, 848 F.3d at 315–16.

Here, as in *El-Masri*, "this question is easily answered in the negative." *El-Masri*, 437 F. Supp. 2d at 539. Any decision or evidentiary hearing on the issue of standing—directed at determining whether communications of Plaintiff were subject to surveillance—by definition would require the Court to adjudicate whether Plaintiff, as an entity, is or was subject to Upstream surveillance activities, a fact that the Court has already identified as being among those "which should not be divulged in the interest of national security." *Wikimedia*, 2018 WL 3973016, at *12. Put another way, if this Court were to adjudicate the issue of standing, "the whole object of the [adjudication] . . . [would be] to establish a fact that is a state secret." *Sterling*, 416 F.3d at 348. For this reason alone, even if Plaintiff could demonstrate an issue of material fact concerning standing, this litigation cannot proceed. *See id.* (affirming dismissal because litigation would have "center[ed] around" methods and operations of the CIA).

Additionally, whether Plaintiff's communications are subject to Upstream surveillance or not, litigating the issue of standing would implicate operational details of Upstream collection that may indirectly bear on the Plaintiff's standing, including: locations at which Upstream surveillance is conducted, categories of Internet-based communications subject to Upstream surveillance activities, and, more broadly, the scope and scale on which Upstream surveillance is or has been conducted. As to all of these categories of information, too, the Court has already found that they "fall[] squarely within the ambit of the state secrets privilege." *Wikimedia*, 2018 WL 3973016, at *12.

Moreover, in light of the determination that the classified information bearing on Plaintiff's standing cannot be disclosed without risk of exceptionally grave damage to national security, the Court should decline any invitation by Plaintiff to probe into or speculate about these classified facts, or to try to piece together, based on publicly available materials, facts that have been removed from the case by the state secrets privilege. In analogous circumstances, in *El-Masri*, this Court

cautioned that nothing in its opinion assessing the Government's assertion of the state secrets privilege should be understood to be "comment[ing] or rul[ing] in any way on the truth or falsity of [plaintiff's] factual allegations." *See* 437 F. Supp. 2d at 540. Having found that the information constituted "matters which, in the interest of national security, should not be divulged," *id.* at 537, the Court expressly avoided placing the imprimatur of judicial fact-finding on plaintiffs' speculation regarding those classified facts, and dismissed the plaintiff's complaint. In the instant case, the Court's determination that disclosure of the above-listed categories of information bearing on Plaintiff's standing "would undermine ongoing intelligence operations, deprive the NSA of existing intelligence methods, and significantly, provide foreign adversaries with the tools necessary both to evade U.S. intelligence operations and to conduct their own operations against the United States and its allies," necessitates the same approach. *Wikimedia*, 2018 WL 3973016, at *12.

CONCLUSION

For the foregoing reasons, Defendants' motion for summary judgment should be granted.

Dated: November 13, 2018

Respectfully submitted,

JOSEPH H. HUNT
Assistant Attorney General

ANTHONY J. COPPOLINO
Deputy Branch Director

/s/ James J. Gilligan
JAMES J. GILLIGAN
Special Litigation Counsel

RODNEY PATTON
Senior Trial Counsel

JULIA A. BERMAN
Senior Counsel

OLIVIA HUSSEY SCOTT
Trial Attorney

U.S. Department of Justice
Civil Division, Federal Programs Branch
1100 L Street, N.W., Room 11200
Washington, D.C. 20005
Phone: (202) 514-3358
Fax: (202) 616-8470
Email: james.gilligan@usdoj.gov

Counsel for Defendants