IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION,	)	
Plaintiff,	)	
	)	
v.	)	**Case No. 1:15-cv-662**
	)	
NATIONAL SECURITY AGENCY/ CENTRAL SECURITY SERVICE, *et al.*,	)	
	)	
Defendants.	)	

MEMORANDUM OPINION

Plaintiff, Wikimedia Foundation ("Wikimedia"),[1] challenges the legality of the National Security Agency's ("NSA") Upstream surveillance data gathering efforts, one of a series of recent cases challenging the constitutionality of the NSA's surveillance programs.[2] According to the Director of National Intelligence ("DNI"), Upstream surveillance is a surveillance program authorized pursuant to § 702 of the Foreign Intelligence Surveillance Act ("FISA") that involves the targeted collection of non-U.S. persons' international Internet communications by the NSA.[3] Wikimedia alleges that the NSA has intercepted, copied, and collected Wikimedia's Internet

---

[1] This action was originally brought by nine organizations, including Wikimedia, that communicate over the Internet. The other eight organizations were dismissed at the threshold because those organizations lacked Article III standing. *See Wikimedia Found. v. Nat'l Sec. Agency*, 857 F.3d 193, 216–17 (4th Cir. 2017) (affirming in part *Wikimedia Found. v. Nat'l Sec. Agency*, 143 F. Supp. 3d 344 (D. Md. 2015)).

[2] *See Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1144 (2013) (involving a facial challenge to Section 702 of the Foreign Intelligence Surveillance Act); *Obama v. Klayman*, 800 F.3d 559 (D.C. Cir. 2015) (involving a challenge to the NSA's bulk collection of telephone metadata produced by telephone companies); *Am. Civil Liberties Union v. Clapper*, 785 F.3d 787 (2d Cir. 2015) (involving a challenge to the NSA's bulk telephone metadata collection program); *Jewel v. Nat'l Sec. Agency*, No. C 08–04373 (N.D. Cal. April 25, 2019), *appeal docketed*, No. 19–16066 (9th Cir. May 21, 2019) (involving a challenge to the NSA's interception of Internet communications); *Schuchardt v. Trump*, 2019 WL 426482 (W.D. Pa. Feb. 4, 2019), *appeal docketed*, No. 19–1366 (3d Cir. Feb. 14, 2019) (involving a challenge to the NSA's interception of Internet communications through the PRISM surveillance program).

[3] *See* Pub. Decl. of Daniel R. Coats, Director of National Intelligence, ¶ 15, ECF No. 138-2.

communications pursuant to the Upstream surveillance program and that such interception, duplication, and collection exceeds the NSA's authority under FISA and violates Wikimedia's rights under the First and Fourth Amendments of the Constitution.

At issue in this matter is defendants' motion for summary judgment. Defendants argue that judgment must be entered in their favor because Wikimedia, the only remaining plaintiff, lacks Article III standing. Defendants also argue that even if a genuine dispute of material fact exists as to Wikimedia's standing, the state secrets doctrine precludes further litigation of Wikimedia's standing, and thus requires entry of judgment in defendants' favor.

Before analyzing the parties' arguments on the issue of Article III standing and the state secrets doctrine, however, it is important to address briefly three topics: (i) the definition of Upstream surveillance and the statutory authority for the NSA's Upstream surveillance program, (ii) the procedural history of this case, and (iii) the undisputed factual record developed by the parties. After addressing these three preliminary topics, which frame all of the analysis that follows, the pertinent summary judgment standard is set forth, and the parties' arguments are analyzed under that standard. For the reasons that follow, Wikimedia has failed to establish that it has Article III standing sufficient to survive summary judgment, and further litigation of this matter is precluded by the state secrets doctrine. Accordingly, this case must be dismissed, and judgment must be entered in favor of defendants.

I.

To begin with, it is necessary to define Upstream surveillance, the NSA program at issue in this litigation, and to clarify what is meant by the term Upstream surveillance as that term is used in this litigation. The NSA conducts Upstream surveillance pursuant to § 702 of FISA, 50 U.S.C. § 1881a. The government has acknowledged that it conducts § 702 surveillance through

two programs, namely the Upstream and PRISM programs.[4] In PRISM surveillance, the government acquires communications directly from a United States-based Internet Service Provider ("ISP"). *See* PCLOB 702 Report, at 33. In contrast, the acquisition of communications via Upstream surveillance does not occur "with the compelled assistance of the United States ISPs, but instead with the compelled assistance...of the providers that control the telecommunications backbone over which communications transit."[5] *Id.* at 35. Thus, Upstream collection, unlike PRISM collection, "does not occur at the local telephone company or email provider with whom the targeted person interacts." *Id.* Instead, the collection of communications for Upstream surveillance "occurs 'upstream' in the flow of communications between communication service providers." *Id.* Only the Upstream surveillance program is at issue in this case.

As noted, the government contends that its Upstream surveillance program is conducted pursuant to FISA § 702. Specifically, § 702 permits the Attorney General and the DNI to authorize jointly, for up to one year, foreign-intelligence surveillance targeted at non-U.S. persons located abroad,[6] if the Foreign Intelligence Surveillance Court ("FISC")[7] approves the government's written certification demonstrating that the intended surveillance complies with statutory

---

[4] *See* Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* 7 (2014) ("PCLOB 702 Report"), *available at* https://www.pclob.gov/library/702-Report-2.pdf.

[5] The telecommunications or Internet "backbone" is the network of high-capacity fiber-optic cables, switches, and routers operated by telecommunications service providers that facilitates both domestic and international communication via the Internet. This backbone primarily consists of a network of fiber-optic cables, including terrestrial cables that link areas across the U.S. and transoceanic cables that link the U.S. to the rest of the world.

[6] Importantly, the statute expressly prohibits the intentional targeting of any persons known at the time of acquisition to be in the United States or any U.S. person reasonably believed to be located outside the United States. 50 U.S.C. § 1881a(b). Section 702 does allow the government, however, to intercept communications between a U.S. person inside the United States and a foreigner located abroad who has been targeted by intelligence officials. *See id.* § 1881a(a)–(b).

[7] FISC, a tribunal composed of eleven federal judges designated by the Chief Justice of the U.S. Supreme Court, is charged with the review of applications for electronic surveillance. *See* 50 U.S.C. § 1803(a).

requirements.[8] To approve such a certification, the FISC must determine that the government's targeting procedures are reasonably designed:

> (i) to ensure that acquisition "is limited to targeting persons reasonably believed to be located outside the United States," 50 U.S.C. § 1881a(j)(2)(B)(i);
>
> (ii) to prevent the intentional acquisition of wholly domestic communications, *id.* § 1881a(j)(2)(B)(ii);
>
> (iii) to "minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign-intelligence information," *id.* § 1801(h)(1); *see id.* § 1881a(j)(2)(C); and
>
> (iv) to ensure that the procedures "are consistent with...the [F]ourth [A]mendment," *id* § 1881a(j)(3)(A).[9]

In effect, FISC approval of government surveillance pursuant to § 702 means that the FISC has found that the surveillance comports with the statutory requirements and the Constitution.

The recent release of public reports and declassification of some FISC opinions have revealed additional details regarding the collection of communications pursuant to § 702. After the FISC approves a § 702 certification, the NSA designates "targets," which are 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.[10] The NSA then attempts to identify "selectors," namely the specific means by which the targets communicate,

---

[8] The government must certify that a significant purpose of the acquisition is to obtain foreign intelligence information and that the acquisition will be conducted in a manner consistent with the Fourth Amendment and the targeting and minimization procedures required by statute. 50 U.S.C. § 1881a(b), (g).

[9] In addition, following the passage of the FISA Amendments Reauthorization Act of 2017, the FISC must now also find that the government's querying procedures meet the statutory requirements and are consistent with the Fourth Amendment. *Id.* § 1881a(j)(2)(D); (j)(3)(A). These provisions have been cited to the version of § 1881a in effect since January 18, 2018. All of these provisions are identical to those in the version of § 1881a effective between June 2, 2015 and January 18, 2018, but the provisions are now located within § 1881a(j) rather than § 1881a(i).

[10] PCLOB 702 Report, at 41–46.

such as email addresses or telephone numbers.[11] Importantly, selectors cannot be key words (*e.g.*, "bomb") or targets' names (*e.g.*, "Bin Laden"); rather, selectors must be specific communication identifiers.[12] The government then may issue a § 702 directive to a U.S. telecommunications service provider requiring it to assist the government in acquiring communications involving those selectors.[13]

As for the actual collection of communications containing these targeted selectors, the government has described the Upstream surveillance collection process as follows:

> [C]ertain 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.

Defs.' Br. 4 (quoting Pub. Decl. of Daniel R. Coats, Director of National Intelligence, ¶ 15, ECF No. 138-2).[14] Thus, the Upstream surveillance collection process involves three steps—(1) filtering, (2) scanning, and (3) ingesting. As this description shows, although the government has disclosed some information about Upstream surveillance in declassified documents and

---

[11] NSA Director of Civil Liberties and Privacy Office Report, *NSA's Implementation of FISA Section 702* 4 (2014), *available at* https://www.nsa.gov/Portals/70/documents/news-features/press-room/statements/NSAImplementationofFISA70216Apr2014.pdf.

[12] *Id.*; PCLOB 702 Report, at 32–33, 36.

[13] 50 U.S.C. § 1881a(i); PCLOB 702 Report, at 32–33.

[14] Prior to April 2017, 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) (emphasis in original), *available at* https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf. According to the PCLOB 702 Report, under the Upstream surveillance program that included "about" collection, "a communication between two third parties might be acquired because it contains a targeted email address in the body of the communication." PCLOB 702 Report, at 119. As of March 2017, however, the NSA ceased "about" collection entirely, which a FISC judge concluded "should substantially reduce the acquisition of non-pertinent information concerning U.S. persons pursuant to Section 702." FISC Mem. Op. & Order, at 23, 25 (April 16, 2017).

unclassified reports, most technical details of the Upstream surveillance process remain classified. *Wikimedia Found. v. Nat'l Sec. Agency*, 857 F.3d 193, 202 (4th Cir. 2017) (citing *Jewel v. Nat'l Sec. Agency*, 810 F.3d 622, 627 (9th Cir. 2015)).

II.

With this statutory framework and definition of Upstream surveillance in mind, it is appropriate to turn to the procedural history of this case. On June 22, 2015, Wikimedia, along with eight other organizations,[15] filed the Amended Complaint in this suit, challenging the legality of the NSA's Upstream surveillance program. The Amended Complaint alleges that Upstream surveillance (i) exceeds the scope of the government's authority under § 702, (ii) violates Article III, (iii) violates the First Amendment, and (iv) violates the Fourth Amendment and requests (i) a declaration that Upstream surveillance violates the Constitution and § 702 and (ii) an order permanently enjoining the NSA from conducting Upstream surveillance. On August 6, 2015, defendants moved to dismiss the Amended Complaint, arguing that plaintiffs lacked Article III standing. On October 23, 2015, defendants' motion was granted on the ground that plaintiffs' allegations were too speculative to establish Article III standing. *Wikimedia Found. v. Nat'l Sec. Agency,* 143 F. Supp. 3d 344, 356 (D. Md. 2015), *aff'd in part, vacated in part, and remanded by*, 857 F.3d 193 (4th Cir. 2017).

Thereafter, plaintiffs appealed, and the Fourth Circuit affirmed in part, vacated in part, and remanded the case for further consideration. *Wikimedia Found.,* 857 F.3d at 200. Specifically, the Fourth Circuit vacated the finding that Wikimedia lacked standing, but affirmed the finding that the other plaintiffs lacked standing. *Id.* The Fourth Circuit concluded that Wikimedia had

[15] These original plaintiffs included the National Association of Criminal Defense Lawyers, Human Rights Watch, Amnesty International USA, Pen American Center, Global Fund for Women, the Nation magazine, the Rutherford Institute, and the Washington Office on Latin America.

established standing sufficient to survive a facial challenge to the Amended Complaint based on the "Wikimedia Allegation", namely the allegation "that the sheer volume of [Wikimedia's] communications makes it virtually certain that the NSA has intercepted, copied, and reviewed at least some of [Wikimedia's] communications[,]" "even if the NSA conducts Upstream surveillance on only a single [I]nternet [backbone] link." *Id.* at 202, 209 (internal quotation marks and citation omitted). Three factual allegations, accepted as true as required at the motion to dismiss stage, made the Wikimedia Allegation plausible: (i) "Wikimedia's communications almost certainly traverse every international [Internet] backbone link connecting the United States with the rest of the world[,]" (ii) "the NSA has confirmed that it conducts Upstream surveillance at more than one point along the [I]nternet backbone[,]" and (iii) "the government, for technical reasons[,] . . . must be copying and reviewing all the international text-based communications that travel across a given [Internet backbone] link upon which it has installed surveillance equipment." *Id.* at 210–11 (internal quotation marks and citations omitted).

Importantly, the Fourth Circuit rejected the "Dragnet Allegation", that is the allegation "that[,] in the course of conducting Upstream surveillance[,] the NSA is intercepting, copying, and reviewing substantially all text-based communications entering and leaving the United States, including" those of the nine plaintiffs. *Id.* at 202 (internal quotation marks and citation omitted). Plaintiffs alleged the following facts in support of the Dragnet Allegation: (i) "the NSA has a strong incentive to intercept communications at as many [Internet] backbone chokepoints as possible, and indeed must be doing so at many different [Internet] backbone chokepoints," (ii) "the technical rules governing online communications make this conclusion especially true," and (iii) "a *New York Times* article asserts that the NSA is temporarily copying and then sifting through the contents of what is apparently most e-mails and other text-based communications that cross the

[U.S.] border." *Id.* at 213 (internal quotation marks and citations omitted). The Fourth Circuit concluded that the Dragnet Allegation failed to establish standing because it did "not contain enough well-pleaded facts entitled to the presumption of truth." *Id.* at 200. As such, although Wikimedia pled sufficient facts to establish standing at the motion to dismiss stage, the other plaintiffs did not. *Id.* at 200. Thus, Wikimedia is the only remaining plaintiff.

On remand, an Order issued on October 3, 2017 directing the parties to conduct a limited five-month period of jurisdictional discovery. *See* ECF Nos. 117, 123. Both sides took depositions and served requests for written discovery and production of documents. Defendants objected to 53 of Wikimedia's 84 discovery requests on the ground that responses to the requests would reveal classified information protected by the common law state secrets privilege and related statutory privileges. Thereafter, the DNI formally asserted the state secrets privilege and the statutory privilege set forth in 50 U.S.C. § 3024(i)(1).[16] Defendants stated that the information Wikimedia sought, if disclosed, reasonably could be expected to result in exceptionally grave damage to U.S. national security.[17] Wikimedia subsequently moved to compel production of the documents. On August 20, 2018, an Order and Memorandum Opinion issued, concluding that defendants satisfied the procedural requirements necessary to invoke the state secrets privilege, that the information sought to be protected qualified as privileged under

[16] Defendants also submitted a classified declaration from George C. Barnes, the Deputy Director of the NSA. The classified declaration provided additional detail about the harm to national security that would be caused by disclosure of the information contained in Wikimedia's discovery requests.

[17] The DNI's and the NSA's assertions of privilege encompassed seven categories of information: (i) individuals or entities subject to Upstream surveillance; (ii) 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); (iii) locations (and nature of the locations) at which Upstream surveillance is conducted; (iv) the specific types or categories of communications either subject to or acquired in the course of the Upstream collection process; (v) the scope and scale on which Upstream collection has or is now being conducted; (vi) the NSA's cryptanalytic capabilities or limitations; and (vii) additional categories of classified information encompassed within numerous FISC opinions and orders. *See* DNI Decl. ¶¶ 18, 21–47.

the state secrets doctrine, and that therefore, Wikimedia's motion to compel must be denied. *Wikimedia Found. v. Nat'l Sec. Agency,* 335 F. Supp. 3d 772, 790 (D. Md. 2018). Accordingly, the parties continued jurisdictional discovery, limited to information not protected by the state secrets privilege.

Defendants now seek summary judgment on the ground that Wikimedia lacks Article III standing to contest the legality of the NSA's Upstream surveillance program, or alternatively, that if there is a genuine issue of material fact as to the three essential elements of the Wikimedia Allegation articulated in the Fourth Circuit's remand order, the state secrets doctrine operates to preclude further litigation of Wikimedia's standing and thus requires entry of judgment in defendants' favor.

III.

Summary judgment is appropriate only where there are no genuine disputes of material fact. Rule 56, Fed. R. Civ. P. Accordingly, the material facts as to which no genuine dispute exists must first be identified. Defendants set out their statement of material facts in their brief in support of summary judgment, as required by the local rules. Plaintiff, in addition to responding to defendants' statement of material facts as required by the local rules, also offered their own separate statement of material facts in their brief in opposition to summary judgment. Neither the local rules of the District of Maryland nor the Eastern District of Virginia require plaintiff, as the non-moving party, to set forth a statement of material facts. *See generally* D. Md. Local Rules; E.D. Va. Local Civ. R. 56(B). In the interest of completeness, however, and because each party has responded to the other party's statement of material facts, all facts, and disputes as to those facts, have been considered in deriving from the record the following undisputed material facts.

1. The Internet is a global collection of networks, large and small, interconnected by

a set of routers.[18] Together, these large and small networks function as a single, large virtual network, on which any device connected to the network can communicate with any other connected device.

2. 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, an Internet café). In turn, the local ISP's network connects to the networks of larger regional and national ISPs, the largest of which are called "Tier 1" telecommunication service providers (*e.g.*, AT&T, CenturyLink, Cogent, Verizon).

3. 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 a nation or region. Data travel across these cables in the form of optical signals, or pulses of light.

4. 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 the terrestrial telecommunications network.

5. Tier 1 providers and other large carriers typically connect separate legs of their own networks using high-capacity switches. To allow users of different providers' networks to communicate with one another, Tier 1 providers and other large carriers typically interconnect their networks using high-capacity routers.[19]

6. Generally speaking, to send a communication on the Internet, the transmitting device (*e.g.*, a personal computer, a cell phone) first converts the communication into one or more small bundles of data called "packets," configured according to globally accepted protocols.[20]

7. When a communication is broken into separate packets, each packet includes (i) a "header," which consists of the routing, addressing, and other technical information required to facilitate the packets' travel from its source to its intended

---

[18] Routers are specialized computers that ensure that Internet communications travel an appropriate path across the Internet. Routers serve a similar role for the Internet as switches (or switchboards) do on the telephone network.

[19] Routers and switches perform similar functions, namely directing the transport of Internet communications across the network. Routers generally connect one communications service provider's network to a different communications service provider's network, whereas switches generally connect a single communication provider's network.

[20] Protocols can be thought of as electronic languages. Each protocol, or language, has its own rules and vocabulary. For example, instead of English and Spanish, there is Transmission Control Protocol ("TCP") and User Datagram Protocol ("UDP").

destination, and (ii) a "payload," which consists of a portion of the contents of the communication being transmitted.

8. 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 ports; and (iii) protocol numbers.

9. IP addresses, which are included in packet headers, are unique numeric identifiers assigned to particular computers, devices, or systems connected to the Internet.[21] IP addresses are used to direct data back and forth between one computer (or other online device) and another online device. IP addresses may be analogized to the destination and return addresses on a mailing envelope.

10. The IP addresses of entities with a large, fixed presence on the Internet do not change and are publicly accessible.[22]

11. Port numbers, which are also included in packet headers, are used to identify communications of different kinds (*e.g.*, webpage requests, or email) so that servers hosting multiple communications services (*e.g.*, a website and an email service) can distinguish packets destined for one service from those meant for another. Port numbers for common applications, like web-browsing and email, are assigned in a common industry registry maintained by the IANA. Whereas 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.

12. Protocol numbers, which are also included in packet headers, are used by receiving devices to determine the appropriate method of interpreting data (*e.g.*, HTTP, TCP/IP). A protocol defines the actions taken upon the transmission and/or receipt of a message or other transmission. Protocols are also assigned numbers maintained in a common industry registry maintained by the IANA.

---

[21] There are circumstances, however, in which IP addresses do not uniquely identify individual Internet users. For example, residential Internet customers ordinarily get exactly one "dynamic" IP address at a time, which is assigned on a temporary basis by their ISP. Dynamic IP addresses may be assigned for a day, an hour, or some other period of time depending on the needs, resources, and business practices of a particular ISP, after which the dynamic IP addresses are assigned to other customers. Thus, although the IP addresses of business customers of ISPs almost never change, the IP addresses of individual ISP customers can change fairly often, with the same IP address subsequently being assigned to a different customer of the ISP. *See* Dr. Henning Schulzrinne Decl. ¶¶ 30, 33-34, ECF No. 162-2. As another example, the IP addresses in the packets that make up email messages sent or received by an email server on behalf of its users may have the IP address of the server as the source or destination IP address, not an IP address associated with the individual email user. In other words, the IP address in packets transmitting email messages might be the IP address of the email server (*e.g.*, Gmail, Yahoo), rather than the IP address of the individual user of the email address. Scott Bradner Decl. ¶¶ 244-46, ECF No. 168-2.

[22] Each Internet Service Provider or other large enterprise with a fixed presence on the Internet (*e.g.*, Amazon, Wikimedia) acquires blocks of "static" IP addresses assigned on a permanent basis from the appropriate regional Internet registry affiliated with the global Internet Assigned Numbers Authority ("IANA"). There are public databases that record, with very high accuracy, which address blocks are used by what entities.

13. After 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.

14. Each router or switch through which a packet transits scans the packet's header information, including its destination IP address, and determines which direction (path) the packet should follow next in order to reach its intended destination. The router or switch operates somewhat similarly to Google Maps, updating the fastest route to take between a user's starting point and his or her destination.

15. When packets transmitting a communication arrive at the receiving computer, smartphone, or other online device, the receiving device reassembles the packets into the original communication, such as a webpage or email.

16. Traffic "mirroring" is a technical term for 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. In other words, traffic mirroring can create a copy of all communications, or a subset of all communications, passing through a router or switch without interrupting the flow of those communications.

17. Traffic mirroring is accomplished by programming routers and switches with access control lists ("ACLs") to determine whether packets will be copied and collected at a certain link (the "interface") between the router or switch and another device. The criteria used in the ACL can include a packet's source or destination IP address, the port number, the protocol numbers, or other information contained in a packet header.

18. 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 without mirroring (copying).

19. Tier 1 providers and other smaller service providers employ traffic mirroring in the normal course of their operations for such purposes as monitoring traffic load, conducting quality-control processes, and rejecting unwanted traffic.

20. At any link on the Internet where surveillance may be conducted, traffic mirroring with ACLs can be used in several ways to make only certain packets available for inspection by a collecting entity.[23]

---

[23] Plaintiff disputes this fact, as well as facts 22-24, to the extent the "collector" or the "collecting entity" is the NSA conducting Upstream surveillance. These facts, as stated, do not put forth that the "collector" or the "collecting entity" is the NSA. In fact, these facts simply establish that any entity, government or private, trying to collect Internet communications could, *hypothetically*, employ traffic mirroring in this manner. Plaintiff's argument that the

21. To conduct traffic mirroring, an interface (a fiber-optic link) would have to be established between the router or switch directing traffic at the selected location and the separate equipment used by the collecting entity (hereinafter, the "collector interface").

22. After the collector interface is established, communications traffic passing through the carrier's router or switch to the collector's equipment can be filtered by "whitelisting" or "blacklisting" techniques. "Whitelisting" or "blacklisting" involves 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.

23. For example, the collector could configure an ACL containing a "whitelist" of specific IP addresses of interest. 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, and 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. In other words, packets containing IP addresses on the whitelist would be copied and sent through to the collector's equipment. Packets not meeting the whitelist criteria would not be copied for, or made available to, the collector's equipment for any purpose.

24. Blacklisting, conversely, involves configuring an ACL to allow all packets to be copied to the collector interface *except* those matching the ACL's criteria. With a blacklist, the router or switch would examine each packet header and (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) create an additional copy of every 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. In other words, if the router or switch finds that a packet header contains a source or destination IP address on the blacklist, an additional copy of that packet is not created or forwarded through the collector interface.

25. Whitelisting and blacklisting techniques can also be used to limit mirroring to particular sources of traffic, such as only cables used by specific carriers, or only cables linked to specific countries or regions.

26. In addition, ACLs can be configured to whitelist or blacklist particular types of communication based on their port or protocol numbers, such as email communications or communications from accessing websites.

NSA does not use traffic mirroring in this way when the NSA conducts Upstream surveillance is discussed at length *infra* Part V.C.

27. Wikimedia operates twelve free-knowledge projects on the Internet, including Wikipedia. Wikipedia, a free-access, free content encyclopedia, is one of the top ten most-visited websites in the world. In 2017, Wikipedia's website received visits from more than 1 billion unique devices each month.

28. Wikimedia engages in more than a trillion international Internet communications each year, with individuals in every country on the planet. This includes communications between foreign users and Wikimedia's U.S.-based servers, and communications between U.S. users and Wikimedia's foreign-based servers.

29. Wikimedia has identified three categories of its international Internet communications that it contends are subjected to Upstream surveillance collection by the NSA: (i) communications with its community members[24] ("Category 1"), (ii) internal "log" communications ("Category 2"), and (iii) the electronic communications of Wikimedia's staff ("Category 3").

30. Category 1 consists of communications with and among Wikimedia's community members, including requests from foreign and domestic users to view or download content from Wikimedia websites, and email communications sent from foreign users to Wikimedia servers.[25] All of these communications were directed to the public IP address ranges assigned to and used by Wikimedia.

31. Category 2 consists of internal log communications transmitted from Wikimedia's servers in the Netherlands to its servers in the United States. These communications are encrypted and received at one of the same public IP address ranges as Wikimedia's communications in Category 1.[26]

32. Category 3 consists of communications by Wikimedia's staff using various protocols, some of which are encrypted, some of which are not. These communications, like those in Categories 1 and 2, are sent and received from the public IP address ranges assigned to and used by Wikimedia.[27]

33. The total volume of Wikimedia's international Internet communications exceeds the number of cables transporting Internet communications between the U.S. and other countries. Moreover, Wikimedia's communications are broadly distributed, with users in every country in the world.

---

[24] Wikimedia community members are people who read or contribute to Wikimedia's twelve free-knowledge projects.

[25] According to Wikimedia, the volume of the email communications in Category 1, and the countries from which those emails are received, are unknown. Defs.' Ex. 4, Pl.'s Am Resps. & Objs. to ODNI Interrog. No. 19, Ex. 1 (hereinafter, "Technical Statistics Chart"), ECF No. 162-5.

[26] Technical Statistics Chart; Schulzrinne Decl. ¶¶ 83-84.

[27] Technical Statistics Chart; Schulzrinne Decl. ¶¶ 85-87.

34. It is "virtually certain" that Wikimedia's communications traverse every cable carrying public Internet traffic that connects the U.S. to other countries.

35. The government has described Upstream surveillance as involving three steps. First, "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." Second, these Internet transactions "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." And third, "those transactions that pass through both the filtering and the scanning are ingested into Government databases."[28]

36. Prior to April 2017, Upstream surveillance involved "about" collection (i.e., a communication containing a reference in the communication's text to a selector tasked for acquisition under § 702). "About" communications were not necessarily sent to or from the user of a § 702 tasked-selector.

37. The statement—the "NSA will acquire a wholly domestic 'about' communication if the transaction containing the communication is routed through an international Internet link being monitored by NSA or is routed through a foreign server"—was accurate as of October 3, 2011.[29]

IV.

Summary judgment is appropriate when there is "no genuine issue as to any material fact" and based on those undisputed facts the moving party "is entitled to judgment as a matter of law." *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986). To serve as a bar to summary judgment, facts must be "material," which means that the disputed fact "might affect the

---

[28] Pub. Decl. of Daniel R. Coats, Director of National Intelligence, ¶ 15, ECF No. 138-2.

[29] R. Richards Dep. at 160:4-17; [Redacted], 2011 WL 10945618, at *15. Defendants' Rule 30(b)(6) witness confirmed the accuracy of this statement as of October 2011. Defendants argue that statements of fact in a judicial opinion, such as this statement from a FISC Opinion, are inadmissible hearsay, and thus, plaintiff cannot rely on such statements at summary judgment. Summary judgement evidence must either be in admissible form or capable of being rendered admissible at trial. *Humphreys & Partners Architects, LP v. Lessard Design, Inc.*, 790 F.3d 532, 538-39 (4th Cir. 2015); Fed. R. civ. P. 56(c)(2). Statements of fact in judicial opinions that are offered for the truth of the matter asserted are hearsay. *Nipper v. Snipes*, 7 F.3d 415, 417-18 (4th Cir. 1993); *see also Zeus Enter., Inc. v. Alphin Aircraft, Inc.*, 190 F.3d 238, 242 (4th Cir. 1999); *Carter v. Burch*, 34 F.3d 257, 265 (4th Cir. 1994). Even though the 2011 FISC Opinion is inadmissible hearsay, defendants' Rule 30(b)(6) witness testimony, confirming the accuracy of this specific statement as of October 3, 2011, is not hearsay. Thus, this statement is admissible, but solely this statement because it is as a statement of a party opponent.

outcome of the suit under the governing law." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). 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 that party will bear the burden of proof at trial," there can be no genuine issue as to any material fact. *Celotex Corp.* 477 U.S. at 322.

Article III limits the jurisdiction of federal courts to actual "Cases" or "Controversies." *See* U.S. Const. art. III, § 2, cl. 1. As the Supreme Court has made clear, one "essential and unchanging part of the case-or-controversy requirement" is that a plaintiff must establish Article III standing to sue. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992). A plaintiff establishes Article III standing by showing that he, she, or it seeks relief from an injury that is "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling." *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147 (2013) (quoting *Monsanto Co. v. Geerston Seed Farms*, 561 U.S. 139, 149 (2010)). In other words, a plaintiff must establish (1) an injury-in-fact; (2) a casual connection between the injury and the alleged conduct; and (3) the redressability of the injury by a court.

To establish injury-in-fact, the alleged injury must be "real and immediate," not "conjectural or hypothetical." *City of Lost Angeles v. Lyons*, 461 U.S. 95, 201 (1983). The Supreme Court has "repeatedly reiterated that '[a] threatened injury must be *certainly impending* to constitute injury in fact,' and that '[a]llegations of *possible* future injury' are not sufficient." *Clapper*, 133 S. Ct. at 1147 (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)) (emphases in original). In some cases, injury-in-fact can also be established "based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably [sic] incur costs to mitigate or avoid that harm."[30] *Id.* at 1150 n. 5. Importantly, the standing inquiry is

[30] The parties disagree on whether the appropriate standard for determining injury-in-fact sufficient to establish

"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 was unconstitutional," particularly "in the fields of intelligence gathering and foreign affairs." *Clapper*, 133 S. Ct. at 1147.

Because standing is a threshold jurisdictional requirement, it may be attacked at any time, including at summary judgment. As the Supreme Court has made clear, each element of standing must be supported "in the same way as any other matter on which the plaintiff bears the burden of proof, *i.e.*, with the manner and degree of evidence required at the successive stages of the litigation." *Defenders of Wildlife*, 540 U.S. at 561. Where, as here, standing is challenged at the summary judgment stage, "'the party invoking federal jurisdiction bears the burden of establishing' standing—and...such a party 'can no longer rest on...mere allegations, but must set forth by affidavit or other evidence specific facts'" to establish standing. *Clapper*, 133 S. Ct. at 1148-49 (quoting *Defenders of Wildlife*, 504 U.S. at 561).

Thus, if a 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,

---

standing is a "certainly impending" standard or a "substantial risk" standard in this case. The Supreme Court has not been clear as to whether the "substantial risk" standard applies and whether that standard is distinct from the "certainly impending" requirement in cases such as this that involve government surveillance. *See Clapper*, 133 S. Ct. at 1150 n. 5. But the Supreme Court has "found standing based on a 'substantial risk' that harm will occur" in some cases. *Id.*

The Fourth Circuit has indicated that injury-in-fact may be established under either the "certainly impending" or the "substantial risk" standard, and thus, standing should be analyzed under both standards in some cases. *See Beck v. McDonald*, 848 F.3d 262, 275 (4th Cir. 2017) (after determining that the threatened harm was not "certainly impending," the Fourth Circuit stated "our inquiry on standing is not at an end, for we may also find standing based on a 'substantial risk' that the harm will occur, which in turn may prompt a party to reasonably [sic] incur costs to mitigate or avoid that harm"). Importantly, the "substantial risk" standard does not change "the common-sense notion that a threatened event can be 'reasonabl[y] likel[y]' to occur but still be insufficiently 'imminent' to constitute an injury-in-fact." *Id.* at 276.

In this opinion, both standards are applied. Moreover, the injury-in-fact standard, whether "certainly impending," "substantial risk," or both, does not impact the outcome in this case because under whichever standard applies, litigation of any remaining dispute of material fact as to Wikimedia's Article III standing cannot be further litigated without violating the state secretes doctrine, as further discussed *infra* Part VI.

then Rule 56(c) mandates entry of summary judgment against the plaintiff. *See Celotex Corp.*, 477 U.S. at 322.

V.

At this stage of the litigation, Wikimedia must present specific facts, supported by admissible record evidence, that are sufficient to show a genuine issue for trial on Wikimedia's Article III standing. In other words, Wikimedia must present specific facts which show that defendants, through the Upstream surveillance program, have copied and collected Wikimedia's international Internet communications, or that such collection is certainly impending, or that there is a substantial risk that collection will occur such that Wikimedia must incur costs to avoid collection.[31]

Both parties have focused their discussion of Wikimedia's standing on the three prongs necessary to establish the Wikimedia Allegation,[32] which were enumerated in the Fourth Circuit's remand order in this case. *See Wikimedia Found.*, 857 F.3d at 210–11. The three prongs are: (A) Wikimedia's communications almost certainly traverse every international Internet backbone link connecting the United States with the rest of the world; (B) the NSA conducts Upstream surveillance at one or more points along the Internet backbone; and (C) the NSA, for technical reasons, must be copying and reviewing all the text-based communications that travel across a given Internet backbone link upon which it conducts Upstream surveillance. Together,

---

[31] *See Obama v. Klayman*, 800 F.3d 559, 562 (D.C. Cir. 2015) ("In other words, plaintiffs here must show *their own* metadata was collected by the government.") (emphasis in original); *Halkin v. Helms*, 690 F.2d 977, 999-1000 (D.C. Cir. 1982) ("[T]he absence of proof of actual acquisition of appellants' communications is fatal to their watchlisting claims.").

[32] The Wikimedia Allegation is the allegation that the sheer volume of Wikimedia's communications makes it virtually certain that the NSA has intercepted, copied, and reviewed at least some of Wikimedia's communications through the Upstream surveillance program, even if the NSA conducts Upstream surveillance on only a single Internet backbone link. *See supra* page 7.

these three prongs would establish that the NSA has copied and collected some of Wikimedia's communications in the course of the NSA's Upstream surveillance program, thereby providing Wikimedia standing to sue here.

The sufficiency of the evidence with respect to each of these prongs is discussed in detail below. The summary judgment record contains specific facts which show no genuine dispute as to the veracity of the first two prongs of the Wikimedia Allegation. With respect to the third prong, however, the summary judgment factual record contains specific facts that establish, without a genuine dispute of material fact, that the NSA, in the course of Upstream surveillance, does not need to be copying any of Wikimedia's communications as a technological necessity. Thus, the summary judgment record does not contain the facts necessary for Wikimedia to establish standing at summary judgment via the Wikimedia Allegation.

A.

The first prong of the Wikimedia Allegation is that Wikimedia's communications almost certainly traverse every international Internet backbone link connecting the United States with the rest of the world.

Wikimedia primarily supports this contention through the declarations of Scott Bradner, plaintiff's Internet expert.[33] Mr. Bradner states that "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), ECF No. 168-2. Mr. Bradner supports this conclusion with evidence of the volume and global distribution of Wikimedia's communications and the relatively few international circuits connecting the U.S. to

[33] Mr. Bradner worked at Harvard University from 1966 to 2016 in a variety of technical and educational roles, including service as Harvard University's Chief Technology Security Officer for a number of years.

other countries. *Id.* at ¶¶ 346-47, 201-05, 209, 218, 220. Thus, Mr. Bradner concludes, to a virtual certainty, that every international fiber-optic cable that transports Internet communications between the U.S. and the rest of the world transports at least some of Wikimedia's international communications.

Defendants have not disputed this fact. *See* Defs.' Brief in Support of Motion for Summary Judgment, Dkt. 162 at 1 (referring to Wikimedia's standing argument as a "one-legged stool" and taking issue with the other two prongs of Wikimedia's standing argument, but not with the argument that Wikimedia's communications traverse every international Internet backbone link).[34]

Thus, there is no genuine dispute between the parties in the summary judgment record that Wikimedia's communications almost certainly traverse every international Internet backbone link connecting the United States with the rest of the world. Wikimedia has presented specific facts, supported by the conclusion of Mr. Bradner, that establish the first prong of the Wikimedia Allegation.

B.

The second prong of the Wikimedia Allegation is that the NSA conducts Upstream surveillance at one or more international Internet backbone links, all of which, as established in the first prong, some of Wikimedia's communications traverse.

Wikimedia primarily relies upon a sentence in a redacted 2011 FISC Opinion and on language describing the Internet backbone in the PCLOB 702 Report to establish this prong. The

---

[34] The government has not explicitly conceded this prong of the Wikimedia Allegation, that Wikimedia's communications traverse every international Internet backbone link connecting the United States with the rest of the world. But the government has indicated that even assuming *arguendo* that Wikimedia has presented sufficient facts to establish this first prong, Wikimedia still does not have standing in this case. *See also id.* at 21.

sentence in the 2011 FISC Opinion states: the "NSA will acquire a wholly domestic 'about' communication if the transaction containing the communication is routed through an international Internet link being monitored by NSA or is routed through a foreign server." [Redacted], 2011 WL 10945618, at *15. Defendants' Rule 30(b)(6) witness confirmed the accuracy of this statement as of October 2011.[35] *See* R. Richards Dep. at 160:4-17. Thus, as a statement of a party opponent, this statement is admitted as part of the summary judgment record.

Based on this admission, plaintiff contends that Upstream surveillance involves monitoring "international Internet link[s]." Defendants, however, assert that the meaning of the term "international Internet link" is protected by the state secrets privilege and cannot be confirmed or denied by defendants. Defendants' Rule 30(b)(6) witness testified that "unlike the other words you had me go through in terms of definitions...[which were] what a teleco[m] expert would" provide, the "NSA has an understanding of this term [international Internet link] that is specific to how [the FISC Judge] described it, but it's classified to provide any further information." R. Richards Dep. at 160:19-161:22. Thus, the differences between the term "international Internet link" and the term "circuits," which is a colloquial term used in the telecom industry and is used to describe where along the Internet backbone Upstream collection occurs in the PCLOB 702 Report,[36] cannot be known without violation of the state secrets

---

[35] *See supra* note 29 for further detail as to why the statement in the 2011 FISC Opinion is not inadmissible hearsay in the context of this litigation as a result of defendants' Rule 30(b)(6) testimony regarding the statement.

[36] It is worth noting that the PCLOB 702 Report's reference to "circuits" does not suggest that the NSA is conducting surveillance on more than one circuit. To be sure, the PCLOB 702 Report does use the term "circuits," but it does not do so to refer to the number of sites the NSA is monitoring. Instead, the PCLOB 702 Report uses the term "circuits" in the context of defining the "Internet backbone." Specifically, the PCLOB 702 Report explains that the "Internet backbone" consists of "circuits that are used to facilitate Internet communications[.]" PCLOB 702 Report at 36-37.

privilege.[37] *See* PCLOB 702 Report, at 35-37. Moreover, that this statement was accurate on October 3, 2011 says nothing of this statement's accuracy either in 2015, when this suit was filed, or today.[38]

Rather than belabor the squabble between the parties about the meaning of this particular term from a 2011 FISC Opinion, a different, admissible record document sheds significantly more light on this prong of the Wikimedia Allegation. The Public Declaration of Daniel R. Coats, Director of National Intelligence ("DNI"), states that the United States Intelligence Community "has publicly acknowledged that Upstream surveillance is conducted on one or more points on the Internet backbone" and that the United States Intelligence Community "has publicly acknowledged that...NSA is monitoring at least one circuit carrying international Internet communications." Pub. Decl. of Daniel R. Coats, DNI, ¶¶ 30, 37, ECF No. 138-2.[39] In other words, the DNI, who oversees the United States Intelligence Community, has admitted, in the course of this litigation, that the NSA conducts Upstream surveillance on at least one point on the Internet backbone and, to the extent the terms Internet backbone and international Internet circuit are not interchangeable, on at least one circuit carrying international Internet communications.[40]

---

[37] The state secrets privilege's applicability to this case is discussed in significantly greater depth *infra* Part VI.

[38] The statement from the 2011 FISC Opinion pertains to the Upstream surveillance program's collection of "about" communications. As of April 2017, Upstream surveillance no longer involves any "about" collection. Thus, at least the conclusion of this conditional statement is no longer accurate today.

[39] Neither party has cited to these specific paragraphs of the Public Declaration of the DNI in their briefs. Nonetheless, the Public Declaration of the DNI is clearly part of the evidentiary record in this matter, as defendants have cited to other paragraphs of this declaration in their statement of undisputed material facts. Moreover, as the "oversee[r of] the United States Intelligence Community," the DNI is in a position to make such statements from personal knowledge.

[40] In this context, the terms Internet backbone and international Internet circuits both refer on some level to the transoceanic fiber-optic cables that transport Internet communications and connect the U.S. to the rest of the world.

Accordingly, the undisputed summary judgment record adequately establishes that the NSA monitors at least one circuit carrying international Internet communications in the course of Upstream surveillance and that Wikimedia's communications traverse every circuit carrying international Internet communications from the United States to the rest of the world. Thus, Wikimedia has established the first two prongs of the Wikimedia Allegation with the support of admissible record evidence and without a genuine dispute as to any material fact.

C.

With respect to the third prong, however, the summary judgment factual record contains specific facts that establish, without a genuine dispute of material fact, that it is *not* a technological necessity that the NSA has copied or collected some of Wikimedia's communications over the one circuit that the NSA admits monitoring to conduct Upstream surveillance.[41] Accordingly, the summary judgment record does not contain the facts necessary for Wikimedia to establish standing at summary judgment via the Wikimedia Allegation.

To address this prong of the Wikimedia Allegation, both parties have submitted extensive expert reports. The government's expert, Dr. Henning Schulzrinne,[42] has provided expert testimony that details a method of collecting Internet communications, which could, *hypothetically*, avoid collecting any of Wikimedia's communications. Dr. Schulzrinne Decl. ¶

---

[41] Importantly, to establish standing, Wikimedia need only prove that the NSA has copied or scanned some of its communications as part of the Upstream surveillance program, or that such collection is certainly impending, or that there is a substantial risk that collection will occur such that Wikimedia must incur costs to avoid collection. Wikimedia has chosen to prove that it is a technological necessity that the NSA has copied or scanned some of its communications only because the government's assertion of the state secrets privilege prevents Wikimedia from posing the more direct question of whether the NSA has actually copied or scanned any of Wikimedia's communications as part of the Upstream surveillance program. *See Wikimedia Found. v. Nat'l Sec. Agency*, 335 F. Supp. 3d 772, 788-90 (D. Md. 2018).

[42] Dr. Henning Schulzrinne has been a professor of computer science at Columbia University since 1996 and holds a Ph.D. and a Master's Degree in Electrical Engineering.

77-88. Thus, Dr. Schulzrinne concludes that the NSA, via Upstream surveillance, does not *have* to be collecting any of Wikimedia's communications "as a matter of technological necessity." Dr. Schulzrinne 2d Decl. ¶ 2. Importantly, Dr. Schulzrinne does not provide testimony about the actual operational details of Upstream surveillance because the actual operational details of Upstream surveillance are classified and protected by the state secrets privilege, and thus, Dr. Schulzrinne does not know any of the classified operational details. *Id.* at ¶ 3-4.

On the other side, Wikimedia's expert, Scott Bradner, has provided expert testimony in which he opines, based on a combination of technical and practical factors, that the NSA "most likely" copies all communications transported across an international Internet circuit *before* filtering any of the communications. Bradner Decl. ¶ 282. As a result, Mr. Bradner concludes that "even if the NSA were monitoring only a single circuit under [U]pstream collection, it would be copying and reviewing at least some of Wikimedia's communications." *Id.* at ¶ 353.

Each expert unsurprisingly takes issue with the other's findings. Dr. Schulzrinne claims that Mr. Bradner has provided "no support, and certainly none based in Internet technology and engineering, for concluding that the NSA 'almost certainly' (Bradner Decl. ¶ 6(a)) copies and scans all communications traversing any circuit it monitors, including Wikimedia's." Dr. Schulzrinne 2d Decl. ¶ 5. And Mr. Bradner claims that Dr. Schulzrinne's conclusion that the NSA does not have to be collecting any of Wikimedia's communications as a matter of technological necessity "is simply implausible as a practical matter given everything that is known about [U]pstream collection." Bradner Decl. ¶ 362. For the reasons that follow, this dispute does not present a triable issue of fact.

To begin with, it is necessary to address the practical grounds on which Mr. Bradner reaches his conclusions. Mr. Bradner contends that the NSA could not accomplish its stated goal

of "*comprehensively acquir[ing]* communications that are sent to or from its targets" through Upstream surveillance without first copying all international communications transported over the circuit(s) that the NSA is monitoring. *Id.* at ¶ 333 (quoting PCLOB 702 Report, at 10, 123, 143 (emphasis added)); *Id.* at ¶ 335. To accomplish this goal, Mr. Bradner opines that the NSA is "most likely" copying all of the communications traveling across a circuit before later filtering those communications based on the NSA's targeted selectors. *Id.* at ¶¶ 282, 289. As the basis for this opinion, Mr. Bradner claims (i) that any other method would require the NSA to share sensitive information about its targets and/or filtering criteria with an assisting provider, which the NSA would prefer not to do, (ii) that any other method would require the NSA to place an NSA-operated device into the heart of an ISP's network, which the NSA would prefer not to do, and (iii) that the NSA has no operational incentive to reduce the number of communications it scans for selectors. *Id.* at ¶¶ 283-88.

None of Mr. Bradner's bases for this opinion, however, have a non-speculative foundation in technology. Instead, speculative assumptions about the NSA's surveillance practices and priorities and the NSA's resources and capabilities form the basis for Mr. Bradner's opinion in this regard.[43] *See* Dr. Schulzrinne 2d Decl. ¶ 73. Simply put, Mr. Bradner does not know what the NSA prioritizes in the Upstream surveillance program because that information is classified, and therefore Mr. Bradner has no knowledge or information about it.

---

[43] *See, e.g., Obama v. Klayman*, 800 F.3d 559, 567 (D.C. Cir. 2015) (rejecting a plaintiff's claim that the NSA's collection must be comprehensive to be effective because "there are various competing interests that may constrain the government's pursuit of effective surveillance. Plaintiffs' inference fails to account for the possibility that legal constraints, technical challenges, budget limitations, or other interests prevented NSA from collecting metadata from Verizon Wireless."). Wikimedia has gone significantly further than the plaintiffs in *Klayman* to address the technological issues pertinent to the effectiveness of a less comprehensive surveillance system, but Mr. Bradner still takes significant speculative leaps about the NSA's practical and operational decision-making to reach these particular aspects of his conclusions. These specific conclusions require speculative leaps which are too significant to accept as the foundational basis for an expert's opinion.

As a result, Mr. Bradner's opinions as to these specific propositions are inadmissible pursuant to Rule 702, Fed. R. Evid., and the standards articulated in *Daubert v. Merrell Pharmaceuticals, Inc.*, 509 U.S. 579 (1993).[44]

Moreover, even if Mr. Bradner's opinions on these specific propositions were admissible, any conclusions drawn from those opinions would be barred by the state secrets doctrine, as further discussed *infra* Part VI. No matter how intuitively appealing Mr. Bradner's opinions about the NSA's operational priorities may seem, courts have consistently recognized that "judicial intuition" about such propositions "is no substitute for [the] documented risks and threats posed by the potential disclosure of national security information." *Al-Haramain Islamic Found., Inc. v. Bush*, 507 F.3d 1190, 1203 (9th Cir. 2007). Importantly, defendants cannot effectively defend themselves against Mr. Bradner's speculations without disclosing information about the operational details of the NSA's Upstream surveillance program. But defendants have thoroughly documented the risks of such a disclosure in the classified declaration, explaining that to reveal such facts regarding the operational details of the Upstream surveillance collection process, even considering the public disclosures made to date, would provide insight into the structure and operations of the Upstream surveillance program and in so doing, undermine the effectiveness of this important intelligence method. Thus, even if Mr. Bradner's conclusions,

---

[44] Rule 702 provides that an expert may offer opinion testimony if "the expert's scientific, technical, or other specialized knowledge" will be helpful to understand the evidence or to determine a fact in issue, the proffered opinion is "based on sufficient facts or data," and it is "the product of reliable principles and methods...reliably applied...to the facts of the case." Fed. R. Evid. 702(a)-(d). *Daubert* explained that to meet the test of admissibility under Rule 702, an expert's testimony must rest on a reliable foundation, meaning it "must be based on scientific, technical, or other specialized *knowledge* and not belief or speculation." *Oglesby v. Gen. Motors Corp.*, 190 F.3d 244, 250 (4th Cir. 1999) (emphasis in original); *see also Nease v. Ford Motor Co.*, 848 F.3d 219, 229, 231 (4th Cir. 2017). Here, the critical propositions that form the basis for Mr. Bradner's opinion that the NSA is "most likely" copying all communications before any filtering do not meet this requirement as they are based on Mr. Bradner's speculation as to the NSA's operational priorities and capabilities, not on any technical requirements for the collection of Internet communications. Although the NSA has made some public disclosures about Upstream surveillance, Mr. Bradner's interpretations of single sentences within the public disclosures stretches those disclosures far beyond a natural reading of them, and again, is not based on any knowledge, technical or otherwise.

built off assumptions about the NSA's operational goals from the NSA's limited public disclosures, were admissible as expert opinions, the state secrets doctrine would bar any further litigation of this prong of Wikimedia's standing argument, as further discussed *infra* Part VI.

Analysis of the third prong of the Wikimedia Allegation, however, does not end with dismissal of Mr. Bradner's non-technical assumptions. Each expert has also presented technical arguments for and against the proposition that the NSA must be collecting at least some of Wikimedia's communications at the circuit(s) monitored pursuant to the Upstream surveillance program.

Dr. Schulzrinne explains how the NSA, using the technique of "traffic mirroring" in a specific manner,[45] could conduct Upstream surveillance on an international Internet circuit "without intercepting, copying, reviewing, or otherwise interacting with [the] communications of Wikimedia." Dr. Schulzrinne Decl. ¶ 77. To begin with, Wikimedia has been allocated a number of static IP addresses. *Id.* at ¶ 80. A "static" IP address is an IP address that is assigned on a *permanent* basis from the appropriate regional Internet registry. *See id.* at ¶ 32-33. Static IP addresses are generally assigned to large enterprises on the Internet so that users around the world have consistent access to their websites. Public databases record, with very high accuracy, which IP address blocks are used by what entities. *Id.* Thus, any member of the public can ascertain all of the IP addresses assigned to Wikimedia.

Through a process of "blacklisting" Wikimedia's IP addresses, the NSA could conduct Upstream surveillance without receiving access to any of Wikimedia's communications. *Id.* at ¶ 82. To do so, the NSA could blacklist all of Wikimedia's IP addresses using an access control

---

[45] Traffic mirroring, as defined in the statement of material facts in the summary judgment record, is a technical term for a process by which all communications passing through a router or switch can be copied without interrupting the flow of communications.

list, a list employed in the traffic mirroring process that determines which packets carrying Internet communications will be copied and collected at a certain circuit on the Internet backbone. By blacklisting Wikimedia's IP addresses, all Internet communications *except* those containing Wikimedia's blacklisted IP addresses would be copied and collected by the NSA. Importantly, this hypothetical does not propose that the NSA is copying all Internet communications other than Wikimedia's, but rather states that, as a technical matter, the NSA *could* blacklist certain high-frequency, low-interest IP addresses to minimize the collection of communications of little interest to the NSA and that Wikimedia's IP addresses *could* be high-frequency, low-interest IP addresses to the NSA. Thus, strictly considering the technological limitations of copying Internet communication in transit, it is possible that the NSA has not copied and collected any of Wikimedia's communications despite monitoring an international Internet circuit that transmits some of Wikimedia's communications.[46]

In response, Mr. Bradner finds this hypothetical "simply implausible" as a practical matter given everything that is known about Upstream surveillance, although Mr. Bradner does admit that selective collection is technologically possible. Bradner Decl. ¶ 362, 272(b), 280-81, 299, 325, 366. The foundation for Mr. Bradner's response is that the NSA has disclosed to the public that Upstream surveillance operates by identifying "selectors," the specific means by which the targets communicate, such as email addresses or telephone numbers.[47] Because the

---

[46] In addition to blacklisting Wikimedia's IP addresses, Dr. Schulzrinne proposes several other whitelisting or blacklisting options which would prevent the NSA from collecting Wikimedia's international Internet communications. Dr. Schulzrinne Decl. ¶ 77-88. For example, the NSA could blacklist the ports assigned to HTTP and HTTPS communications so as not to collect any web communications that involve accessing websites. *Id.* at ¶ 79.

[47] NSA Director of Civil Liberties and Privacy Office Report, *NSA's Implementation of FISA Section 702* 4 (2014), *available at* https://www.nsa.gov/Portals/70/documents/news-features/press-room/statements/NSAImplementationofFISA70216Apr2014.pdf.

NSA cannot know in advance which communications contain selectors, Mr. Bradner contends, the NSA must first copy all communications before scanning any of them for selectors. Bradner Decl. ¶ 333, 301.

Despite Mr. Bradner's arguments to the contrary, the traffic mirroring hypothetical proposed by Dr. Schulzrinne does not contradict the government's public disclosures about Upstream surveillance. Importantly, the government has described Upstream surveillance as involving three steps—(1) filtering, (2) scanning, and (3) ingesting.[48] The whitelisting and blacklisting process of traffic mirroring proposed by Dr. Schulzrinne would occur at the first step in the NSA's collection process, the filtering, prior to any copying or scanning. Thus, under Dr. Schulzrinne's hypothetical, the first step, filtering, would involve a combination of whitelisting and blacklisting to exclude wholly domestic communications *and* other low interest communications, and Wikimedia's communications may qualify as low interest communications that the NSA filters out.[49] *Second*, and only after filtering, the NSA would scan the remaining communications for "selectors," which could result in the collection of both communications to or from a targeted selector and about a targeted selector. *See* Dr. Schulzrinne 2d Decl. ¶ 50-52. This second step described in the government's public disclosures is the step on which Mr. Brander focuses. Given the distinction between the first two steps, Dr. Schulzrinne's hypothetical is consistent with government's public disclosures about Upstream surveillance.

---

[48] *See* Material Fact 35; Pub. Decl. of Daniel R. Coats, Director of National Intelligence, ¶ 15, ECF No. 138-2.

[49] It is noted that the government has not disclosed that anything other than wholly domestic communications are filtered out at the first step in the Upstream collection process. Given the government's limited disclosures about the technical details of how Upstream surveillance operates, however, this disclosure does not mean that the government does not, or could not, engage in additional filtering at the first step in the Upstream surveillance collection process. Whether or not the government actually engages in additional filtering at the first step in the Upstream surveillance collection process is a fact protected by the state secrets privilege. *See Wikimedia Found. v. Nat'l Sec. Agency*, 335 F. Supp. 3d 772, 789-90 (D. Md. 2018); Pub. Decl. of Daniel R. Coats, DNI, ¶ 18(B), 18(D), ECF No. 138-2.

Moreover, the hypothetical, regardless of whether it is actually how the NSA conducts Upstream surveillance, does show that there is a technological method by which the NSA could conduct Upstream surveillance on a circuit transporting International internet communications without copying, collecting, or otherwise reviewing any of Wikimedia's communications that traverse that path.

But this does not end the analysis, for there is a technological hurdle that remains. Even if the NSA used the whitelisting and blacklisting techniques proposed by Dr. Schulzrinne to filter the communications it collected via Upstream surveillance, Mr. Bradner maintains that there are three scenarios in which Wikimedia's communications would still be copied and scanned by the NSA. Bradner Decl. ¶¶ 367(b), 370. In these three specific scenarios—namely (i) communications contained within a multi-communication transaction,[50] (ii) emails to or from Wikimedia involving a person located abroad who is using an email service located in the U.S.,[51] or (iii) a person located abroad who accesses Wikimedia's websites through a U.S.-based Virtual

---

[50] A "multi-communication transaction" (MCT) is "an Internet transaction that contain[s] multiple discrete communications." NSA Response to Plaintiff's Interrogatory No. 8 (Dec. 22, 2017). When an email user logs into their email service to check his or her email, the group of all unread email messages is transmitted together as a single communication from the email service to the subscribing user's inbox. This transmission of multiple emails in a single communication might be considered an MCT. Bradner Decl. ¶¶ 67, 132, 317. In transit, an MCT of this type would contain the IP address of the email service as the sender and the IP address of the user as the recipient. If an email to or from Wikimedia were contained within the batch of emails sent as an MCT, the Wikimedia email would be transmitted to the user's inbox without Wikimedia's IP address in the individual packet headers of the MCT. Dr. Schulzrinne 2d Decl. ¶ 78. Thus, this specific type of Wikimedia communication could be transmitted from an email service to a user of the email service without Wikimedia's IP address being the source or destination IP address. And as a result, blacklisting Wikimedia's IP addresses would not prevent the NSA's collection of such an email from an international Internet circuit which the NSA is monitoring.

[51] This scenario is similar to the first MCT scenario. If (i) an email user sent an email to Wikimedia or received an email from Wikimedia, (ii) that email user was abroad, and (iii) that email user utilized a U.S.-based email service, the communication between the email user and the email service would not include Wikimedia's IP address in the packet headers and would need to traverse an international Internet circuit between the U.S.-based email service and the user located abroad. Bradner Decl. ¶ 367(b)(2); Dr. Schulzrinne 2d Decl. ¶ 81. Thus, this specific type of Wikimedia communication could be transmitted from an email service to a user of the email service without Wikimedia's IP address being the source or destination IP address. And as a result, blacklisting Wikimedia's IP addresses would not prevent the NSA's collection of such an email from an international Internet circuit which the NSA is monitoring.

Private Network (VPN),[52] Wikimedia's IP address would not appear as the source or destination IP address on the packet header traversing the international Internet circuit into or out of the U.S. *See* Bradner Decl. ¶ 367(b)(1)-(3); Dr. Schulzrinne 2d Decl. ¶ 77-87. Thus, these communications would not be blocked by the NSA's hypothetical blacklist of Wikimedia's IP addresses because the communications would not contain Wikimedia's IP address in the packet header, despite involving a Wikimedia communication.

Dr. Schulzrinne admits that each of these scenarios is "theoretically possible" but "could come to pass only in the uncertain event that particular conditions are met." Dr. Schulzrinne 2d Decl. ¶ 77. For communications in each of these three scenarios to be collected by the NSA through Upstream surveillance, at least four conditions would have to be met,[53] none of which Wikimedia has established as to any of their communications in this case. Specifically, for Wikimedia communications to exist in either of the first two scenarios, an email user in a foreign location must be downloading emails from a server located in the United States (such that the communication would traverse an international Internet circuit monitored by the NSA) *and* the email user must be sending email to and/or receiving email from Wikimedia. *Id.* at ¶¶ 78, 81. Wikimedia has not presented evidence of any such subset of its communications.[54] For

---

[52] When a user communicates via a Virtual Private Network (VPN), all of the user's communications are encrypted and first routed through the VPN server before being directed to their ultimate destination. Dr. Schulzrinne 2d Decl. ¶ 57. As a result, first, each communication's packet is assigned the VPN server's address as its destination IP address, not the IP address of the ultimate destination. *Id.* Then, once the communication has reached the VPN server (destination one), the communication travels from the VPN server to the ultimate destination (destination two), with the VPN server IP address as the source IP address, rather than the individual user's IP address. Therefore, if a person is located abroad and accesses Wikimedia's website while using a U.S.-based VPN and the first leg communication between the VPN user and the VPN server traverses an international Internet circuit that the NSA is monitoring, the NSA could collect that communication even if the NSA has blacklisted Wikimedia's IP addresses. Bradner Decl. ¶ 367(b)(3).

[53] Dr. Schulzrinne 2d Decl. ¶ 78, 81, 83.

[54] It is worth noting that Wikimedia has acknowledged that is does not know the volume of its international email communications, or the countries from which the emails are received. *See* Technical Statistics Chart. In addition to

Wikimedia's communications to exist in the third scenario, a user of a Virtual Private Network (VPN) that is based in the United States must use that VPN while abroad to visit one of Wikimedia's websites, and the NSA must monitor the international Internet circuit that transmits that communication from the user abroad to the domestic VPN. Again, Wikimedia has not presented evidence of any such subset of its communications. As a result, satisfaction of the chain of conditions necessary to establish that the NSA collected Wikimedia's communications in one of these three circumstances is too speculative to establish standing. *See Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1148, 1150 (2013) (holding that a speculative chain consisting of five contingencies was insufficient to establish standing). Thus, although it is possible that such communications exist,[55] the summary judgment record does not contain any evidence that such communications actually exist, a requirement at this stage of the litigation. *See Clapper*, 133 S. Ct. at 1148-49.

In sum, the undisputed summary judgment record does not establish that the NSA has copied any of Wikimedia's international Internet communications in the course of Upstream surveillance, or that such collection is certainly impending, or that there is a substantial risk that collection will occur such that Wikimedia must incur costs to avoid collection. Specifically, the summary judgment record establishes that it is not a technological necessity that the NSA must copy all of the text-based Internet communications traversing a circuit that the NSA monitors while conducting Upstream surveillance. The NSA could, *hypothetically*, utilize a process of

---

the total volume and location of all of Wikimedia's international email communications being unknown, this particular subset of Wikimedia's international email communications is also unknown – in volume, in geographic diversity, or even whether such communications exist.

[55] It is worth noting that if such communications exist, they are likely to be far fewer in number than the trillions of international Wikimedia communications every year that traverse every International circuit connecting the U.S. to the rest of the world. Thus, a finding that such communications exist could trigger a re-evaluation of the first prong of Wikimedia's standing argument, *i.e.* that Wikimedia's subject international Internet communications traverse every international Internet backbone link connecting the United States with the rest of the world.

whitelisting and blacklisting to filter out low-interest Internet communications, including Wikimedia's communications, prior to scanning the Internet communications for targeted selectors. At most, there is a genuine dispute of material fact as to whether the NSA can conduct Upstream surveillance without copying Wikimedia's communications, if any, that (i) are contained within a multi-communication transaction, (ii) are emails to or from Wikimedia involving a person located abroad using an email service located in the U.S., or (iii) involve a person located abroad accessing Wikimedia's websites through a U.S.-based Virtual Private Network (VPN) *and* that traverse an NSA-monitored circuit. To the extent there is a genuine issue of material fact with respect to the NSA's collection of this currently unidentified subset of Wikimedia's international communications, that issue cannot be further litigated given the state secrets doctrine, as further discussed *infra* Part VI.

VI.

Even assuming *arguendo* that, there is a genuine dispute of material fact as to the third prong of the Wikimedia Allegation, the question remains as to how the matter should proceed consistent with Supreme Court and Fourth Circuit precedent regarding the state secrets doctrine. Wikimedia's standing cannot be fairly litigated any further without disclosure of state secrets absolutely protected by the United States' privilege. For Wikimedia to litigate the standing issue further, and for defendants to defend adequately in any further litigation, would require the disclosure of protected state secrets, namely details about the Upstream surveillance program's operations. For the reasons that follow, therefore, the standing issue cannot be tried, or otherwise further litigated, without risking or requiring harmful disclosures of privileged state secrets, an outcome prohibited under binding Supreme Court and Fourth Circuit precedent. Thus, the case must be dismissed, and judgment must be entered in favor of defendants.

A.

It is necessary first to review the well-settled Supreme Court and Fourth Circuit precedent concerning the state secrets doctrine. Settled Supreme Court and Fourth Circuit precedent make clear that "[u]nder the state secrets doctrine, the United States may prevent the disclosure of information in a judicial proceeding if 'there is a reasonable danger' that such disclosure 'will expose...matters which, in the interest of national security should not be divulged.'" *Abilt v. CIA*, 848 F.3d 305, 310-11 (4th Cir. 2017) (quoting *El-Masri v. United States*, 479 F.3d 296, 302 (4th Cir. 2007)) (quoting *United States v. Reynolds*, 345 U.S. 1, 10 (1953)). In this regard, the Fourth Circuit has recognized that the state secrets doctrine "performs a function of constitutional significance, because it allows the executive branch to protect information whose secrecy is necessary to its military and foreign-affairs responsibilities." *Id.* at 312 (quoting *El-Masri*, 479 F.3d at 303).

The Fourth Circuit has mandated a three-step analysis for resolution of the state secrets question:

> First, "the court must ascertain that the procedural requirements for invoking the state secrets privilege have been satisfied." Second, "the court must decide whether the information sought to be protected qualifies as privileged under the state secrets doctrine." Third, if the "information is determined to be privileged, the ultimate question to be resolved is how the matter should proceed in light of the successful privilege claim."

Abilt, 848 F.3d at 311 (quoting *El-Masri*, 479 F.3d at 304). Previously, an Order and Memorandum Opinion issued in this case, which concluded that defendants satisfied the procedural requirements necessary to invoke the state secrets privilege, that the information sought to be protected qualified as privileged under the state secrets doctrine, and that therefore, Wikimedia's motion to compel certain information in discovery had to be denied. *Wikimedia Found. v. Nat'l Sec. Agency,* 335 F. Supp. 3d 772, 790 (D. Md. 2018). The seven categories of

information determined to be privileged under the state secrets doctrine in relation to plaintiff's motion to compel discovery are the same categories of information at issue for plaintiff to establish standing via further litigation of this case.[56] Thus, as already established in the previous Memorandum Opinion and Order, the first two steps of the state secrets analysis have been resolved, and the step that remains is "how the matter should proceed in light of the successful privilege claim." *Abilt*, 848 F.3d at 311.

B.

How the matter should proceed turns on the centrality of the privileged information to the issue at hand. Whether the NSA has copied and collected any of Wikimedia's international Internet communications, or such collection is certainly impending, or there is a substantial risk that collection will occur such that Wikimedia must incur costs to avoid collection, is the threshold issue for Wikimedia to establish standing in this litigation. Where, as here, the privileged information is so central to the subject matter of the litigation, dismissal is the appropriate, and only available, course of action.

As the Fourth Circuit has made quite clear, "both Supreme Court precedent and our own cases provide that when a judge has satisfied himself [or herself] that the dangers asserted by the government are substantial and real, he [or she] need not—indeed, should not—probe further." *Sterling v. Tenet*, 416 F.3d 338, 345 (4th Cir. 2005). Moreover, Fourth Circuit precedent establishes 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

---

[56] The seven categories of information privileged pursuant to the state secrets doctrine are: (i) individuals or entities subject to Upstream surveillance activities, (ii) operational details of the Upstream collection process, (iii) locations at which Upstream surveillance is conducted, (iv) categories of Internet-based communications subject to Upstream surveillance activities, (v) the scope and scale on which Upstream surveillance is or has been conducted, (vi) the NSA's cryptanalytic capabilities, and (vii) additional categories of classified information contained in FISC opinions, orders and submissions.

privileged matters, dismissal is the appropriate remedy." *El-Masri v. Tenet*, 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).[57]

As such, "[i]f a proceeding involving state secrets can be fairly litigated without resort to the privileged information, it may continue." *El–Masri*, 479 F.3d at 306. On the other hand, "a proceeding in which the state secrets privilege is successfully interposed must be dismissed if the circumstances make clear that privileged information will be so central to the litigation that any attempt to proceed will threaten that information's disclosure." *Id.* at 308 (citations omitted).[58] Such a decision is never taken lightly, as "dismissal is appropriate '[o]nly when no amount of effort and care on the part of the court and the parties will safeguard privileged material.'" *Sterling*, 416 F.3d at 348 (quoting *Fitzgerald v. Penthouse Int'l, Ltd.*, 776 F.2d 1236, 1244 (4th Cir. 1985)) (alteration in original). Nonetheless, "dismissal follows inevitably when the sum and substance of the case involves state secrets." *Id.* at 347. In this regard, the Fourth Circuit has identified three examples of circumstances in which the privileged information is so central to the litigation that dismissal is required. First, "dismissal is required if the plaintiff cannot prove the *prima facie* elements of his or her claim without privileged evidence." *Abilt*, 848 F.3d at 313-14 (citing *Farnsworth Cannon, Inc. v. Grimes*, 635 F.2d 268, 281 (4th Cir. 1980) (en banc) (per curiam)). Second, "even if the plaintiff can prove a *prima facie* case without resort to privileged information, the case should be dismissed if 'the defendants could not properly defend themselves without using privileged evidence.'" *Id.* at 314 (quoting *El-Masri*, 479 F.3d at 309).

---

[57] Importantly, "state secrets and military secrets are equally valid bases for invocation of the evidentiary privilege." *Sterling*, 416 F.3d at 343 (internal quotation marks and alterations omitted).

[58] *See also Sterling*, 416 F.3d at 347–48 ("We have long recognized that when 'the very subject of [the] litigation is itself a state secret,' which provides 'no way [that] case could be tried without compromising sensitive military secrets,' a district court may properly dismiss the plaintiff's case." (quoting *Fitzgerald*, 776 F.2d at 1243) (alterations in original)); *Bowles v. United States*, 950 F.2d 154, 156 (4th Cir. 1991) (per curiam) ("If the case cannot be tried without compromising sensitive foreign policy secrets, the case must be dismissed.").

Third, "dismissal is appropriate where further litigation would present an unjustifiable risk of disclosure" of state secrets. *Id.* (citing *El-Masri*, 479 F.3d at 308).

C.

Given these principles and given "the delicate balance to be struck in applying the state secrets doctrine," it is appropriate to analyze the litigation at hand, namely the centrality of state secrets to Wikimedia's standing. *El-Masri*, 479 F.3d at 308. To establish standing, Wikimedia must prove (1) injury-in-fact, (2) causation, and (3) redressability. Through an extensive jurisdictional discovery process, Wikimedia has established that the NSA monitors at least one circuit carrying international Internet communications in the course of Upstream surveillance and that Wikimedia's communications traverse every circuit carrying international Internet communications from the United States to the rest of the world. Importantly, this extensive jurisdictional discovery process has resulted in the compilation of a voluminous record, including hundreds of pages of expert reports, government disclosures and declassified documents regarding Upstream surveillance, Rule 30(b)(6) testimony from an NSA representative, and extensive interrogatory responses from the parties. Thus, Wikimedia has been granted the opportunity to establish its standing without resort to privileged information, and Wikimedia has made significant progress on that front.

Nonetheless, the summary judgment record does not establish that the NSA has copied or collected any of Wikimedia's communications via Upstream surveillance conducted on an NSA-monitored circuit, that such collection is certainly impending, or that there is a substantial risk that collection will occur such that Wikimedia must incur costs to avoid collection. Wikimedia has been unable to make this showing because it is not true, as a technological necessity, that the NSA must be copying every text-based communication that traverses a circuit that the NSA

monitors. Indeed, Dr. Schulzrinne has convincingly demonstrated that there are technologically feasible methods by which the NSA could hypothetically operate Upstream surveillance that would result in the NSA not copying or collecting any of Wikimedia's communications. Thus, the undisputed summary judgment record establishes that Wikimedia does not have Article III standing sufficient to survive summary judgment.

Even if Wikimedia could establish a *prima facie* case of its standing based solely on the public, unclassified record, which it has not been able to do thus far in this case, the state secrets doctrine still requires dismissal because the defendants cannot properly defend themselves without using privileged evidence. The Fourth Circuit "ha[s] consistently upheld dismissal when the defendants could not properly defend themselves without using privileged information." *Abilt v. CIA*, 848 F.3d 305, 316 (4th Cir. 2017). As in *El-Masri*, "virtually any conceivable response to [Wikimedia's] allegations [that the NSA has copied and collected some of Wikimedia's international Internet communications] would disclose privileged information." *El-Masri*, 479 F.3d at 310. Defendants have provided a detailed and persuasive explanation, in more than 60 pages of classified declarations, that disclosure of the entities subject to Upstream surveillance activity and the operational details of the Upstream collection process would (i) undermine ongoing intelligence operations, (ii) deprive the NSA of existing intelligence operations, and significantly, (iii) 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. *Wikimedia Found. v. Nat'l Sec. Agency*, 335 F. Supp. 3d 772, 789 (D. Md. 2018). Accordingly, defendants could not properly defend themselves in any further litigation of Wikimedia's standing, and thus, the case must be dismissed.

Moreover, if the issue of Wikimedia's standing were further adjudicated, "the whole

object of the [adjudication]...[would be] to establish a fact that is a state secret," presenting an unjustifiable risk of disclosing privileged information. *Sterling*, 416 F.3d at 348. Courts have concluded that where, as here, the information sought to be disclosed involves the identity of parties whose communications have been acquired, this information is properly privileged. *See Al-Haramain Islamic Found., Inc. v. Bush*, 507 F.3d 1190, 1203-04 (9th Cir. 2007) (finding that the fact of a plaintiff's surveillance by the NSA was covered by the state secrets privilege); *Halkin v. Helms*, 598 F.2d 1, 9 (D.C. Cir. 1978) (upholding assertion of state secrets privilege with respect to "the identity of particular individuals whose communications have been acquired"). Accordingly, because the privileged information, namely the operational details of the Upstream collection process and whether any of Wikimedia's international Internet communications have been copied or collected by the NSA, is so central to the litigation of Wikimedia's standing, the case must be dismissed, and judgment must be entered in favor of defendants.

VII.

To avoid the conclusion that the case must be dismissed, Wikimedia revives its argument that 50 U.S.C. § 1806(f) displaces the state secrets doctrine in cases challenging electronic surveillance pursuant to FISA and provides for *in camera* review of the materials related to the NSA's Upstream surveillance program. This argument, however, has already been considered and rejected in this litigation. *See Wikimedia Found. v. Nat'l Sec. Agency,* 335 F. Supp. 3d 772, 786 (D. Md. 2018). Specifically, the "§ 1806(f) procedures do not apply where, as here, a plaintiff has not yet established that it has been the subject of electronic surveillance" as required by the statute. *Id.* at 780. Nonetheless, plaintiff raises two additional arguments as to why *in camera* review pursuant to § 1806(f) is appropriate in this case: (i) plaintiff has now established a

genuine dispute of material fact concerning its status as an "aggrieved person"[59] before invoking FISA's procedures and (ii) the Ninth Circuit recently held that § 1806(f) displaces the state secrets privilege in an affirmative legal challenge to electronic surveillance pursuant to FISA. *See Fazaga v. Fed. Bureau of Investigation*, 916 F.3d 1202 (9th Cir. 2019).

First, plaintiff has not established a genuine dispute of material fact concerning its status as an aggrieved person, *i.e.*, that plaintiff's communications have been the subject of electronic surveillance, as discussed *supra* Part V.C. As previously explained, "the text of § 1806(f) points persuasively to the conclusion that Congress intended § 1806(f) procedures to apply only after it became clear from the factual record that the movant was the subject of electronic surveillance." *Wikimedia Found.*, 335 F. Supp. 3d at 781. To be sure, "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." *Id.* at 784. But here, despite the extensive jurisdictional discovery undertaken in this case, plaintiff has been unable to make a factual showing that Wikimedia was the subject of electronic surveillance using admissible record evidence. Thus, the §1806(f) *in camera* review procedures remain inapplicable to this case.

In addition, no binding authority establishes that § 1806(f)'s review procedures displace the state secrets doctrine even if a plaintiff survived summary judgment on the issue of whether plaintiff has been the target of electronic surveillance, which again is not the case here. Specifically, in *ACLU Foundation of Southern California v. Barr*, 952 F.2d 457 (D.C. Cir. 1991), the D.C. Circuit reasoned that "legitimate concerns about compromising ongoing foreign

---

[59] For the purposes of FISA, an "aggrieved person" is "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance." 50 U.S.C. § 1801(k).

intelligence investigations" are more properly considered at the summary judgment stage, not upon the pleadings. *Id.* at 469. In doing so, the D.C. Circuit only considered what a party must show to establish his or her "aggrieved person" status and therefore invoke § 1806(f) review. Simply put, the D.C. Circuit did not consider whether or when § 1806(f) *in camera* review is inappropriate or unnecessary because of the state secrets doctrine.

Moreover, the Ninth Circuit's opinion in *Fazaga* does not hold that § 1806(f) displaces the state secrets doctrine in this case, despite plaintiff's arguments to the contrary. The Ninth Circuit reasoned in *Fazaga* that § 1806(f)'s procedures displace a dismissal remedy for the *Reynolds* state secrets doctrine *only where § 1806(f)'s procedures apply.*[60] *Fazaga*, 916 F.3d at 1234. Specifically, the Ninth Circuit held that for FISA's § 1806(f) procedures to apply, "[p]laintiffs must satisfy the definition of an 'aggrieved person.'" *Id.* at 1238. In this case, as previously discussed at length, Wikimedia has not established it is an "aggrieved person" as defined in § 1801(k). *See Wikimedia Found. v. Nat'l Sec. Agency,* 335 F. Supp. 3d 772, 780, 786 (D. Md. 2018). Thus, § 1806(f) does not apply to this case, and dismissal on state secrets grounds is appropriate, as discussed *supra* Part VI.

Notably, the only court to address this issue post-*Fazaga* held that "where the very issue

---

[60] *Fazaga* addressed a challenge to an allegedly unlawful FBI counter-terrorism investigation involving electronic surveillance. *Id.* at 1210-11. Specifically, in that case, "several sources" confirmed the identity of a confidential FBI informant and disclosed that that specific confidential informant "created audio and visual recordings" for the FBI. *Id.* at 1214. The district court dismissed all but one of plaintiff's claims at the pleading stage without further discovery based on the government's assertion of the state secrets privilege. *Id.* at 1211. The Ninth Circuit reversed, concluding that § 1806(f)'s procedures are to be used when "aggrieved persons" challenge the legality of electronic surveillance and that the district court erred by dismissing the case without reviewing the evidence. *Id.* at 1238, 1252. In remanding for further proceedings, the *Fazaga* court held that "[t]he complaint's allegations are sufficient *if proven* to establish that Plaintiffs are 'aggrieved persons.'" *Id.* at 1216 (emphasis added). Thus, the Ninth Circuit's decision reasoned that at the pleading stage of the litigation, where plaintiffs have alleged sufficient facts, assumed to be true at that stage of the litigation, to establish they are "aggrieved persons" as required for application of Section 1806(f), dismissal on the basis of the state secrets doctrine was inappropriate. This holding says nothing, however, about the relationship between § 1806(f) and the state secrets doctrine dismissal remedy where, as here, a plaintiff has not established that he, she, or it is an "aggrieved person" using admissible record evidence, after a lengthy jurisdictional review process, at the summary judgment stage of the litigation.

of standing implicates state secrets," the holding in *Fazaga* and § 1806(f) do not foreclose "dismissing [the case] on state secrets grounds" at the summary judgment stage of the litigation.[61] *Jewel v. Nat'l Sec. Agency*, No. C 08–04373, at *24 (N.D. Cal. April 25, 2019), *appeal docketed*, No. 19–16066 (9th Cir. May 21, 2019). Accordingly, because plaintiff has not established it is an "aggrieved person" as defined in the statute, and hence § 1806(f) does not apply, and because the issue of standing in this case necessarily implicates state secrets, dismissal of the case is appropriate.

VIII.

To avoid dismissal of the litigation on state secrets grounds, Wikimedia has raised several additional standing arguments separate and apart from the Wikimedia Allegation—namely (i) Upstream surveillance has impaired Wikimedia's communications with its community members, (ii) Upstream surveillance has required Wikimedia to take costly protective measures, and (iii) Wikimedia has third-party standing to assert the rights of its users. Wikimedia's arguments fail as to each of these theories of standing for the reasons discussed below.

First, Wikimedia argues it has standing because Upstream surveillance has impaired Wikimedia's communications with its community members, as evidenced by a drop in the readership of certain Wikipedia pages. In *Clapper* and *Laird*, however, the Supreme Court unequivocally held that "[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." *Clapper v. Amnesty*

---

[61] To be sure, the district court in California did review "classified evidence submitted by Defendants in response to Plaintiffs' discovery requests" pursuant to the procedures of § 1806(f) of FISA prior to its summary judgment ruling dismissing the case. *Id.* at *24-25. That court did not, however, consider the question of whether plaintiffs were "aggrieved persons" prior to undertaking § 1806(f)'s procedures for *in camera* review. Nevertheless, that court still found that where, as here, "the answer to the question of whether a particular plaintiff was subjected to surveillance – *i.e.*, is an 'aggrieved person' under Section 1806(f) – is the very information over which the Government seeks to assert the state secrets privilege," dismissal of the case and entry of judgment in favor of the government is the appropriate action at summary judgment. *Id.* at *23, *25.

Int'l USA, 133 S. Ct. 1138, 1152 (2013) (quoting *Laird v. Tatum*, 408 U.S. 1, 13-14 (1972)). To avoid the conclusion that any drop in readership is the result of a "subjective chill," Wikimedia relies upon a statistical analysis performed by Dr. Jonathon Penny, which concludes it is "highly likely" that "public awareness of NSA surveillance programs, including Upstream surveillance,...ha[s] had a large-scale chilling effect on Wikipedia users" since June 2013. Dr. Jonathon Penney Decl. ¶ 10-11. But Dr. Penney's conclusion that Wikipedia's readership has suffered an actual chill as the result of Upstream surveillance is undermined for two principal reasons. First, Dr. Penney's data only covers a 32-month period which ends in August 2014, before this lawsuit was even filed. Thus, Dr. Penney's evidence, even if reliable, does not say anything about any ongoing harm suffered by Wikimedia that is traceable to Upstream surveillance. Second, these alleged readership effects were from public awareness of "media coverage of NSA surveillance" generally, not Upstream surveillance specifically. *Id.* at ¶ 26. Thus, Dr. Penney's findings do not demonstrate an ongoing and sustained drop in Wikimedia's readership stemming from the NSA's Upstream surveillance program.

Moreover, "a 'chilling effect aris[ing] merely from the individual's knowledge that a governmental agency was engaged in certain activities or from the individual's concomitant fear that, armed with the fruits of those activities, the agency might in the future take some other and additional action detrimental to that individual'" is insufficient to establish standing.[62] *Clapper*, 133 S. Ct. at 1152 (quoting *Laird*, 408 U.S. at 11). This is exactly the situation here—Wikimedia claims that this decreased readership is a result of individual's fear that the government might be

---

[62] It is worth noting that the Fourth Circuit and the Supreme Court have explained that "standing requirements are somewhat relaxed in First Amendment cases." *Cooksey v. Futrell*, 721 F.3d 226, 235 (4th Cir. 2013) (citing *Secretary of State of Md. v. Joseph H. Munson Co., Inc.*, 467 U.S. 947, 956 (1984)). Even though the standing requirements are somewhat relaxed in the First Amendment context, subjective and speculative fears of government surveillance, such as in this case, do not establish Article III standing at summary judgment, as the Supreme Court specifically held in *Clapper* and *Laird*. *See Clapper*, 133 S. Ct. at 1151-52; *Laird*, 408 U.S. at 10-15.

monitoring their Internet activity and might use that information at some later date. Moreover, the Supreme Court has specifically found that a claimed reluctance by third parties to communicate with a plaintiff, due to their subjective fears of surveillance, is not fairly traceable to the alleged surveillance, and is thus foreclosed as a basis for standing. *Clapper*, 133 S. Ct. at 1152 n.7. Accordingly, Wikimedia cannot establish standing under this theory given the Supreme Court's holdings in *Clapper* and *Laird.*

Second, Wikimedia argues it has standing because Upstream surveillance has required Wikimedia to take costly protective measures—namely, transitioning its Internet communications into encrypted formats such as HTTPS and IPSec, acquiring new technical infrastructure, and hiring a full-time engineer to manage the protective measures. The Supreme Court has already foreclosed this alternative theory of standing where, as here, a plaintiff has failed to establish that their communications have been collected by the government, or that such collection is certainly impending. *Clapper*, 133 S. Ct. at 1151. Applicable here is the Supreme Court's statement in *Clapper* that a plaintiff "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Id.*

Wikimedia attempts to distinguish this case from *Clapper* by arguing that the harm Wikimedia faces from Upstream surveillance is well-established, not some "hypothetical future harm." As discussed at length *supra* in Part V, however, the summary judgment record does not establish that Wikimedia's communications have been collected by the NSA during Upstream surveillance, or that such collection is certainly impending, or that there is a substantial risk that collection will occur such that Wikimedia must incur costs to avoid collection. Thus, any harm to Wikimedia from the Upstream surveillance program remains a purely hypothetical harm

insufficient to establish standing. As the Supreme Court has sensibly observed, to find otherwise "would be tantamount to accepting a repackaged version of [plaintiff's] first failed theory of standing," namely the Wikimedia Allegation. *Id.* (citing *Am. Civil Liberties Union v. Nat'l Sec. Agency*, 493 F.3d 644, 655–56 (6th Cir. 2007)). Accordingly, Wikimedia's alleged expenditures to protect its communications from Upstream surveillance collection do not establish its standing.[63]

Third, Wikimedia argues it has third party standing to assert the rights of its users. In the Fourth Circuit, a plaintiff must demonstrate "(1) an injury-in-fact; (2) a close relationship between [itself] and the person whose right [it] seeks to assert; and (3) a hindrance to the third party's ability to protect his or her own interests" to "overcome the prudential limitation on third-party standing."[64] *Freilich v. Upper Chesapeake Health Inc.*, 313 F.3d 205, 215 (4th Cir. 2002) (citing *Powers v. Ohio*, 499 U.S. 400, 410–11 (1991)). Wikimedia has met none of these requirements. As discussed at length *supra* in Part V, Wikimedia has been unable to establish injury-in-fact in this case. In addition, Wikimedia has not presented admissible evidence that establishes a "close relationship" between Wikimedia and its largely unidentified contributors.[65]

---

[63] Moreover, without evidence that the alleged injuries from implementing these protective measures would be redressed by the injunctive relief plaintiff seeks, these alleged injuries cannot confer standing to sue. *See Clapper*, 568 U.S. at 409; *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992). Given the number of other reasons that plaintiff has admitted influenced its decision to implement these protective measures, including protecting against individual computer hackers and keeping their company policies up-to-date and transparent, injunctive relief enjoining the NSA from conducting the Upstream surveillance program would not redress any alleged injury from these protective expenditures. In fact, Wikimedia began the process of switching to HTTPS as early as 2011, years before any disclosures about the NSA's Upstream surveillance program. *See* ECF No. 178-8.

[64] As the Supreme Court has appropriately warned, "[f]ederal courts must hesitate before resolving a controversy, even one within their constitutional power to resolve, on the basis of the rights of third persons not parties to the litigation." *Singleton v. Wulff*, 428 U.S. 106, 113 (1976).

[65] Close relationships that have established third-party standing in the past include lawyer-client and doctor-patient. *See Department of Labor v. Triplett*, 494 U.S. 715 (1990) (lawyer-client); *Singleton v. Wulff*, 428 U.S. 106 (1976) (doctor-patient). Wikimedia's relationship with its unidentified contributors clearly does not rise to the level of those protected, close relationships.

In fact, Wikimedia has only presented declarations from one single contributor who has edited Wikimedia's web projects while abroad, and this single contributor has stated that her "workload as a medical student" makes it "impossible" for her to bring a lawsuit as a plaintiff.[66] Such "normal burdens of litigation," however, are insufficient to satisfy the third requirement that an obstacle exists that prevents the third party from bringing the lawsuit herself or himself.[67] *See Lawyers Ass'n v. Reno*, 199 F.3d 1352, 1364 (D.C. Cir. 2000). Thus, Wikimedia has also failed to satisfy the third requirement to establish third-party standing. Accordingly, Wikimedia's third-party standing argument clearly fails.

For the reasons stated above, Wikimedia's three additional standing arguments clearly fail because Wikimedia has not established an injury-in-fact using admissible record evidence and Wikimedia has not satisfied the strict requirements to proceed on the basis of third-party standing.

IX.

In sum, Wikimedia has failed to present specific facts which show that defendants, through the Upstream surveillance program, have copied and collected Wikimedia's international Internet communications, that such collection is certainly impending, or that there is a substantial risk that collection will occur such that Wikimedia must incur costs to avoid collection. More specifically, the summary judgment record establishes that it is not a technological necessity that the NSA must copy all of the text-based Internet communications

---

[66] Temple-Wood Decl. ¶ 26, ECF No. 168-10.

[67] Thus, Ms. Temple-Wood, a contributor to Wikimedia's free-knowledge projects, also states that "serving as a plaintiff in a lawsuit would threaten the anonymity [upon which Wikimedia] users depend." Temple-Wood Decl. ¶ 27, ECF No. 168-10. Although privacy and anonymity are valid concerns, in this case a putative plaintiff would not need to reveal the contents of their communications with Wikimedia in order to serve as a plaintiff; they would only need to disclose the form in which the communications were sent (*i.e.*, sending an email or accessing or editing a web project), and the location from which the communications were sent.

traversing a circuit that the NSA monitors while conducting Upstream surveillance. Thus, there is no genuine dispute of material fact that the NSA could conduct Upstream surveillance without collecting any of Wikimedia's communications, and Wikimedia has been unable to present specific facts that establish otherwise, largely because the necessary facts are protected by the state secrets privilege.

Moreover, even if Wikimedia had established a genuine issue of material fact as to whether the NSA has copied or collected any of its international Internet communications, which Wikimedia has not done on this record, further litigation of this matter is precluded by the state secrets doctrine, which has been properly invoked by defendants. The extensive jurisdictional discovery process in this case has made clear that the very issue of standing implicates state secrets and that despite plaintiff's valiant efforts, establishing standing solely on the basis of the public, unclassified record is not possible in this case. Pursuant to Supreme Court and Fourth Circuit precedent, at this stage of the litigation, namely summary judgment post-jurisdictional discovery, dismissal and entry of judgment in favor of defendants is the appropriate, and only available, remedy because the issue of standing in this case necessarily implicates state secrets.

It is important to acknowledge the unfortunate burden that this decision places on Wikimedia. *See Abilt*, 848 F.3d at 317; *Sterling*, 416 F.3d at 348; *El-Masri*, 479 F.3d at 313 ("As we have observed in the past, the successful interposition of the state secrets privilege imposes a heavy burden on the party against whom the privilege is asserted."). Wikimedia suffers dismissal of its claim "not through any fault of [its] own, but because [its] personal interest in pursuing [its] civil claim is subordinated to the collective interest in national security." *El-Masri*, 479 F.3d at 313; *see also Abilt*, 848 F.3d at 318; *Fitzgerald*, 776 F.2d at 1238 n.3 ("When the state secrets privilege is validly asserted, the result is unfairness to individual litigants—through the loss of

important evidence or dismissal of a case—in order to protect a greater public value."). It is appropriate, however, "in limited circumstances like these, [that] the fundamental principle of access to court must bow to the fact that a nation without sound intelligence is a nation at risk." *Sterling*, 416 F.3d at 348.

Plaintiff contends that a holding which finds plaintiff does not have standing and precludes further litigation of this matter because of defendants' invocation of the state secrets doctrine leads to the result that "the Executive Branch alone controls who can and cannot challenge unlawful surveillance."[68] This contention is incorrect; the Supreme Court addressed and rejected a similar argument in *Clapper*. There, the Supreme Court explained that Section 702 surveillance orders are not insulated from judicial review because (i) the FISC reviews the government's certifications, targeting procedures, and minimization procedures for Section 702 surveillance, including whether the targeting and minimization procedures comport with the Fourth Amendment, (ii) criminal defendants prosecuted on the basis of information derived from Section 702 surveillance are given notice of that surveillance and can challenge its validity, and (iii) electronic communications service providers directed to assist the government in surveillance may challenge the directive before the FISC. *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1154 (2013). Even if those other avenues for judicial review were not available, the Supreme Court has made clear that "'[t]he assumption that if [plaintiff has] no standing to sue, no one would have standing, is not a reason to find standing.'" *Id.* (quoting *Valley Forge Christian College v. Americans United for Separation of Church and State, Inc.*, 454 U.S. 464, 489 (1982)).

Moreover, since this litigation began in 2015, FISA Section 702, pursuant to which the

---

[68] Plaintiff's Br. in Op. to Defs.' Motion for Summary Judgment, ECF No. 168, at 2.

NSA Upstream surveillance program operates, was reauthorized by Congress. FISA Section 702 was set to expire on December 31, 2017, but Congress voted in January 2018 to extend FISA Section 702 for an additional six years (the "FISA Amendment Reauthorization Act of 2017").[69] This reauthorization process sparked significant public debate, and the FISA Amendment Reauthorization Act of 2017 enacted a number of reforms to address the public's civil liberties concerns.[70]

Thus, rather than the executive branch alone controlling who can and cannot challenge unlawful surveillance, the judicial branch provides for review and oversight via the limited avenues outlined by the Supreme Court in *Clapper*, including the significant role of the FISC, and the legislative branch provides for review and oversight via the FISA reauthorization process and the executive branch's ongoing reporting requirements to Congress. These avenues are sufficient to meet Constitutional requirements while at the same time precluding the unnecessary disclosure of state secrets.

* * *

For the reasons set forth above, this case must be dismissed, and judgment must be entered for defendants.

An appropriate order will issue separately.

---

[69] FISA Amendments Reauthorization Act of 2017, PL 115-118, January 19, 2018, 132 Stat 3.

[70] For example, the FISA Amendment Reauthorization Act of 2017 added a requirement that the DNI adopt procedures consistent with the requirements of the Fourth Amendment for querying information collected pursuant to Section 702 authority and made these querying procedures subject to FISC review. *See id.* at Sec. 101 Querying Procedures Required. The FISA Amendment Reauthorization Act of 2017 also restricted the use of U.S. person information obtained under Section 702 as evidence in a criminal proceeding and amended the mandatory reporting requirements to require the release of information on the breakdown of U.S. and non-U.S. person targets of electronic surveillance. *See id.* at Sec. 102. These represent only a few of a number of reforms enacted by the FISA Amendment Reauthorization Act of 2017. These reforms, combined with the short period of reauthorization, demonstrate the legislative branch's focused oversight of the executive branch's Section 702 authority.

The Clerk is directed to provide a copy of this Opinion to all counsel of record.

Alexandria, Virginia
December 13, 2019

/s/
T. S. Ellis, III
United States District Judge