IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

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

REPLY BRIEF IN SUPPORT OF DEFENDANTS' MOTION FOR SUMMARY JUDGMENT

Dated: February 15, 2019

JOSEPH H. HUNT
Assistant Attorney General

ANTHONY J. COPPOLINO
Deputy Branch Director

JAMES J. GILLIGAN
Special Litigation Counsel

RODNEY PATTON
Senior Trial Counsel

JULIA A. BERMAN
Senior Counsel

OLIVIA HUSSEY SCOTT
Trial Attorney

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

Counsel for Defendants

TABLE OF CONTENTS

PAGE

PAGE

TABLE OF AUTHORITIES

CASES **PAGE(S)**

PAGE(S)

PAGE(S)

STATUTES

FEDERAL RULES OF CIVIL PROCEDURE

INTRODUCTION

Plaintiff's actions speak louder than its words. "Wikimedia clearly has standing," Plaintiff insists, because it is a "virtual certainty," Plaintiff repeats over and over throughout its brief, that the NSA copies and scans for selectors at least some of its online communications. ECF No. 168 ("Pl.'s Opp."), at 1, 6, 7, 8, 12, 13, 14, 15, 20. One might expect such unqualified expressions of conviction to be paired with a summary judgment motion of Plaintiff's own, yet none is to be seen.

Also no longer to be seen is the theory of the case that Plaintiff steadfastly advanced for nearly four years in this Court and the Fourth Circuit: that as a matter of technological necessity the NSA "must be" copying and scanning all communications transiting any Internet backbone link it allegedly monitors, including Wikimedia's. Without so much as a word of acknowledgment, Plaintiff abandons the centerpiece of its case, and goes so far as to reprimand Defendants and their expert for even bringing it up. The ground to which Plaintiff now retreats, however, is no firmer.

First, as Defendants showed before and demonstrate again here, Plaintiff has presented no admissible evidence that the NSA conducts Upstream surveillance at "international Internet links," and so cannot establish that Upstream surveillance occurs at the links its communications transit (much less that they are copied or scanned there). The equivocal statements contained in the FISC opinion on which Plaintiff relies are inadmissible hearsay. For this reason alone, Defendants are entitled to summary judgment.

Second, it is now conceded by Plaintiff's own Internet technology expert that it is *not* necessary for the NSA, as a technological matter, to copy and scan all communications transiting any Internet backbone link the NSA hypothetically might be monitoring. Plaintiff instead relies on its expert's views that nevertheless the NSA "most likely" does so, and that use of "whitelisting" and "blacklisting" techniques that could avoid interaction with Wikimedia's communications is "implausible." But the Court need only scratch the surface of these opinions to discover that they do not rest on specialized knowledge or information about Internet technology, but on speculation

and belief about NSA surveillance practices and priorities, its resources and capabilities, and the nature and number of its Upstream surveillance targets. These are all classified matters about which Plaintiff's expert has no knowledge or expertise. As a result, these opinions of Plaintiff's expert are inadmissible under the standards of *Daubert v. Merrell Pharmaceuticals, Inc.*, 509 U.S. 579 (1993), leaving no admissible evidence to support Plaintiff's newfound contention that the NSA "most likely" copies and scans its communications. For this reason, too, Defendants are entitled to judgment.

Even if Plaintiff could raise a genuine issue of material fact as to its standing, the entire aim of a trial would be to prove the existence of a fact – whether Wikimedia's communications are subject to Upstream surveillance – that the Court has already ruled is a state secret. And if that were not already the case, any attempt by Plaintiff to prove its standing at trial, even on the basis of admissible public evidence, would almost certainly compromise extraordinarily sensitive information concerning the operational details, locations, and scope and scale of Upstream surveillance, also matters this Court has held are privileged state secrets. None of these outcomes is permitted by the state secrets doctrine. Nor is adjudication of Plaintiff's standing under the procedures of 50 U.S.C. § 1806(f), which, as the Court ruled, has no application until after a litigant has established that it has been a subject of surveillance. Judgment must be entered for Defendants on these grounds, as well.

Finally, absent proof that Plaintiff's communications have been copied and scanned by the NSA, an alleged "chill" on communications with its "community members," and the "protective measures" it has taken to address its community members' concerns, are insufficient as a matter of law to establish Plaintiff's standing. Plaintiff presents no statistically valid evidence of a chilling effect, and any such chill flows only from subjective fears of surveillance among Wikimedia's community members. Under *Clapper v. Amnesty, Int'l USA*, 568 U.S. 398 (2013), neither these fears, nor measures allegedly taken by Wikimedia to address them, are traceable to Upstream surveillance. Plaintiff's third-party standing arguments also lack merit. At bottom, Plaintiff has offered no legally cognizable basis on which its claims can proceed.

RESPONSE TO PLAINTIFF'S STATEMENT OF MATERIAL FACTS

Neither the local rules of the District of Maryland nor of the Eastern District of Virginia required Plaintiff, which has not moved for summary judgment, to set forth a statement of material facts, Pl.'s Opp. at 3-9. *See generally* D. Md. Local Rules; E.D. Va. Local Civ. R. 56(B). Thus, no response to Plaintiff's statement is required here. In the event one is deemed necessary, Defendants provide a response in Appendix A hereto.

ARGUMENT

I. PLAINTIFF MISCONSTRUES ITS LEGAL BURDEN

As a threshold matter, Plaintiff attempts to dilute the legal standard it must satisfy in order to seek prospective relief. Relying on *Susan B. Anthony List v. Driehaus*, 573 U.S. 149 (2014), Plaintiff insists that it need show only a substantial risk that *any* of its Internet communications will be copied or reviewed under Upstream surveillance. Pl.'s Opp. at 13-14. This is not the law.

A plaintiff seeking prospective relief must "establish an ongoing [injury] or [a] future injury in fact," *Abbott v. Pastides*, 900 F.3d 160, 176 (4th Cir. 2018). If the injury in fact is ongoing, it must be "actual," and "not conjectural," *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016). And if the injury is threatened but has not occurred, it must be "certainly impending," *Amnesty Int'l*, 568 U.S. at 409, "real and immediate," and "not conjectural or hypothetical." *City of Los Angeles v. Lyons*, 461 U.S. 95, 102 (1983). Under *Susan B. Anthony List*, 573 U.S. at 158, in certain circumstances a plaintiff may also establish a future injury in fact by demonstrating there is a "substantial risk that the harm will occur." *Beck v. McDonald*, 848 F.3d 262, 275 (4th Cir. 2017). But this is not such a case.

As precedent for the substantial risk standard, *Susan B. Anthony List* cited *Amnesty International*, 568 U.S. at 414 n.5, which made clear that the substantial risk standard applies only when a defendant's "actual action" creates a substantial risk of harm to the plaintiff, prompting the plaintiff to take mitigating measures against the threatened injury. By way of example, *Amnesty International* discussed *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 153-55 (2010), in which the

countermeasures conventional alfalfa farmers took to offset the "substantial risk" of gene flow from genetically modified alfalfa planted nearby was held "readily attributable" to the Government's prior act of deregulating the genetically modified varieties. *See also Beck*, 848 F.3d at 275-76 (applying the "substantial risk" standard to determine whether the Government's action—the loss of a laptop containing personal identifying information—had created a substantial risk of future identity theft).

Here, Plaintiff misapplies the "substantial risk" standard to lower its burden of proof. It is not enough, as Plaintiff maintains, to show "a substantial risk" that its "Internet communications *will be* copied or reviewed under Upstream surveillance." Pl.'s Opp. at 13. Rather, even if the "substantial risk" standard had any application here at all (and it does not), Plaintiff still would have to show that the NSA is engaged in "actual action" (copying and scanning Wikimedia's communications) that creates a "substantial risk" of harm to Wikimedia. To hold otherwise would usher in a lower burden for establishing standing, in much the same way as the Second Circuit's "objectively reasonable likelihood" standard would have done in *Amnesty International*. The Supreme Court emphatically rejected that lower standard, 568 U.S. at 410, 415-16, and this Court should do likewise when it is hidden within the Trojan horse of a "substantial risk" standard.

II. PLAINTIFF HAS NOT RAISED A TRIABLE ISSUE OF MATERIAL FACT CONCERNING NSA INTERACTION WITH ITS COMMUNICATIONS.

A. Plaintiff Lacks Admissible Evidence that the NSA Conducts Upstream Surveillance at International Internet Links Traversed by Wikimedia Communications.

In their initial brief, Defendants showed that Plaintiff lacks evidence to support its allegation that the NSA conducts Upstream surveillance at one or more international Internet links, ECF No. 166 ("Defs.' Br.") at 21-22, a "key fact[]" upon which its standing depends, *see Wikimedia Foundation v. NSA*, 857 F.3d 193, 210-11 (4th Cir. 2017), and which is also classified, and privileged, *see Wikimedia Found. v. NSA*, 335 F. Supp. 3d 772, 788-90 (D. Md. 2018). In an effort to establish this classified fact through public evidence, Plaintiff proffers a single statement from a 2011 FISC

opinion, and its expert's conjecture that it would "make[ ] sense" to conduct Upstream at those sites. Neither is sufficient to create a genuine issue of material fact.

The FISC stated in a 2011 opinion concerning Upstream surveillance that "the government readily concedes that NSA will acquire a wholly domestic 'about' communication *if* the transaction containing the communication is routed through an international Internet link being monitored by NSA." [Redacted], 2011 WL 10945618, at *15 (F.I.S.C. Oct. 3, 2011) (citing a June 1, 2011, Government filing) (emphasis added). Plaintiff argues that this statement constitutes official acknowledgment that Upstream surveillance is conducted "on at least one 'international Internet link.'" Pl.'s Opp. at 16. The FISC's conditional statement, however, is a far cry from confirmation that the NSA was in fact conducting Upstream surveillance at "international Internet links" in 2011, let alone that it continued to do so years later when this case was filed in 2015, or does so now.

Plaintiff also forgets that at summary judgment 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). The FISC's opinion is not admissible because statements of fact in judicial opinions that are offered for the truth of the matters 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 if the opinion were admissible, the statement attributed to the Government concerning "international Internet links" is not. Plaintiff moved to compel Defendants to admit whether it had made such a statement in the filing cited by the FISC, but Defendants asserted the state secrets privilege over that information, an assertion the Court upheld, *Wikimedia*, 335 F. Supp. 3d at 788-90, thus removing it from the case. *El-Masri v. United States*, 479 F.3d 296, 306 (4th Cir. 2007). [1]

[1] Plaintiff also contends that the Government has "declassified" evidence about the "locations" where Upstream surveillance is conducted in the PCLOB's Section 702 Report, which explains that Upstream collection occurs on "circuits" facilitating "the flow of communications between communications service providers." Pl.'s Opp. at 12. This statement says nothing, however, about international Internet links.

Plaintiff also refers to a remark by its Internet technology expert that it would "make[ ] sense" for the NSA to conduct its Upstream surveillance at international Internet links, because they are rich in international traffic of the kind the NSA is authorized to collect. *See* Pl.'s Opp. at 6, 16; *see also* Decl. of Scott Bradner, ECF No. 168-2 ("Bradner Decl.") ¶ 225. What makes sense when it comes to executing the NSA's intelligence mission is not a matter within Mr. Bradner's field of expertise—a subject addressed at greater length *infra*, § II.B—and so his assumption about where it makes sense for the NSA to conduct Upstream surveillance is also inadmissible. Fed. R. Evid. 702.

B. Plaintiff Has Presented No Admissible Evidence That the NSA "Most Likely" Copies and Scans All International Communications, Including Wikimedia's, at Any Internet Backbone Link It May Monitor.

The second key allegation on which Plaintiff for nearly the past four years has based its standing claim is the assertion that the NSA, "for technical reasons," "must be" copying and scanning all the international, text-based communications that travel across a given link it monitors. *Wikimedia*, 857 F.3d at 210-11; *see* Am. Compl. ¶ 62, ECF No. 72. Plaintiff still has offered no evidence to support this allegation, and as Defendants have shown, it is wrong. Defs.' Br. at 22-28. As Defendants' expert, Dr. Henning Schulzrinne, explains, "there are a number of technically feasible, readily implemented means of conducting Upstream-type surveillance that would not require interception, copying, [or] reviewing … all communications that traverse any Internet backbone link the NSA allegedly monitors." 1st Schulzrinne Decl. ¶ 53, ECF No. 166-2. These include "traffic-mirroring" techniques known as "whitelisting" and "blacklisting," *id.* ¶¶ 65-71, which would make it technically feasible to conduct Upstream surveillance in a number of ways that could avoid copying, scanning, or otherwise interacting with Plaintiff's communications, *id.* ¶¶ 77-81.

Plaintiff makes no effort to reclaim the ground on which it once staked its standing claim, that the NSA "must be" copying and scanning all communications that cross a monitored link, including Wikimedia's, as a matter of technological necessity. Indeed, Plaintiff's own expert acknowledges that it is "technically possible" to copy and scan only a subset of the communications

crossing a monitored link whose source or destination IP addresses, or port or protocol numbers, meet specified criteria. Bradner Decl. ¶¶ 7(c), 272(b), 280-81, 299, 325, 366. Despite this concession, Plaintiff still argues, based on Mr. Bradner's declaration, that it is "'virtually certain'" the NSA copies and scans at least some of its communications. Pl.'s Opp. at 15 (quoting *id.* ¶ 6(e)).

Starting from the assumptions that Wikimedia's communications traverse every "international Internet link" with the United States, and that the NSA in fact monitors at least one or more such links, Bradner Decl. ¶¶ 6(d), 225, 291, Mr. Bradner finds it a "virtual certainty" that the NSA copies and scans for selectors at least some of Wikimedia's communications, based on his opinions (i) that the NSA "most likely" copies and scans for selectors all communications packets traversing an international Internet link it monitors (a "copy-all-then-scan" approach); (ii) that it is "implausible" that the NSA uses the traffic-mirroring techniques described by Dr. Schulzrinne; and (iii) that even if the NSA uses one or more of those techniques, it is still "virtually certain" that the NSA copies and scans at least some of Wikimedia's communications. *Id.* ¶¶ 282-89, 366-67, 370.

As is evident from the face of Mr. Bradner's declaration, and confirmed by Dr. Schulzrinne, none of the foregoing opinions expressed by Mr. Bradner has a non-speculative basis in Internet technology. Each is based on speculation about the NSA's surveillance practices and priorities, its resources and capabilities, and the number, nature, and habits of the NSA's Upstream surveillance targets, all classified matters about which Mr. Bradner has no specialized knowledge or information. Defs.' Exh. 6, (Second) Decl. of Dr. Henning Schulzrinne ("2d Schulzrinne Decl.") ¶¶ 3, 4, 14-87. As such, regardless of Mr. Bradner's stated expertise in Internet technology and network design, *see* Bradner Decl. ¶¶ 9-18, his opinions are inadmissible under Federal Rule of Evidence 702, and the standards articulated in *Daubert v. Merrell Pharmaceuticals, Inc.*, 509 U.S. 579 (1993).

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," *Nease v. Ford Motor Co.*, 848 F.3d 219, 229 (4th Cir. 2017) (quoting *Daubert*, 509 U.S. at 597), 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*, 848 F.3d at 231. The critical opinions that inform the "certainty" of Mr. Bradner's conclusions do not meet this requirement.

1. Mr. Bradner's opinion that the NSA "most likely" conducts Upstream surveillance using his copy-all-then-scan approach is without basis in Internet technology or engineering.

Mr. Bradner gives four reasons for considering his copy-all-then-scan approach[2] more likely than the filter-then-copy-and-scan techniques described by Dr. Schulzrinne: (a) that whitelisting or blacklisting would require the NSA to share sensitive information about its targets and/or filtering criteria with an assisting provider, Bradner Decl. ¶¶ 283, 285-87; (b) that whitelisting or blacklisting to reduce the volume of communications that must be scanned for selectors would be of little operational benefit to the NSA, *id.* ¶ 288; (c) that his suggested copy-all-then-scan configuration would not require the placement of "an NSA-operated device into the heart of [a provider's] network," *id.* ¶ 284; and (d) that whitelisting or blacklisting could create a risk of "overloading" the provider's router, *id.* ¶¶ 288, 366(c). We discuss each reason in turn.

a. The extent to which the NSA is willing (or finds it necessary) to share classified information with an assisting provider in order to conduct Upstream surveillance is a classified matter about which Mr. Bradner has no specialized knowledge or information. Uninformed assumptions he may make on that subject are not a basis on which to form a conclusion, from a

[2] Mr. Bradner refers to this process as a "copy-then-filter" configuration, and to the traffic-mirroring described by Dr. Schulzrinne as "in-line filtering." Bradner Decl. ¶¶ 270(b), 272(a), 280-89. For clarity of distinction, Defendants refer to Mr. Bradner's approach as "copy-all-then-scan," and to traffic-mirroring as "filter-then-copy-and-scan." *See* 2d Schulzrinne Decl. ¶ 16.

technological perspective, about the manner in which the NSA conducts Upstream surveillance. 2d Schulzrinne Decl. ¶ 18. Moreover, Mr. Bradner's premise is called into doubt by the fact that the NSA already shares sensitive information about its surveillance targets with assisting provider(s), specifically, the selectors (such as targets' e-mail addresses and telephone numbers) used to identify their communications for acquisition. *See* PCLOB Section 702 Report at 36.

b. Similarly, so far as the operational benefits of filtering traffic before copying and scanning are concerned, whether the NSA places greater importance on the potential intelligence value of scanning every communication that crosses a given link, or the operational efficiencies and cost-savings that would flow from first filtering out communications of low interest, is again a matter about which Mr. Bradner has no knowledge. *See* 2d Schulzrinne Decl. ¶ 19.[3]

c. The major premise of Mr. Bradner's assumption that a *provider* would prefer his copy-all-then-scan approach is that the configuration suggested by Dr. Schulzrinne would involve placement of "an NSA-operated device into the heart of [the provider's] network." Bradner Decl. ¶ 284. But Dr. Schulzrinne made no such proposal. 2d Schulzrinne Decl. ¶¶ 23-24. Plaintiff cannot create a genuine issue of material fact by taking issue with propositions Defendants have not made.

d. Finally, whether the data-processing demands of white- or blacklisting would "overload[ ]" the capacity of a provider's router, Bradner Decl. ¶ 288, would depend in large part on the number of IP addresses (or address blocks) that the NSA designates for white- or blacklisting, which in turn would be significantly related to the number of the NSA's Upstream targets. These are also classified matters about which Mr. Bradner has no knowledge or information.[4]

Thus, Mr. Bradner offers no reliable technical basis on which to conclude that it is "most likely" the NSA follows his "copy-all-then-scan" approach. 2d Schulzrinne Decl. ¶ 29.

---

[3] Moreover, Mr. Bradner significantly underestimates the practical benefits to be gained from first filtering out low-interest communications. *See* 2d Schulzrinne Decl. ¶¶ 19-22.

[4] Mr. Bradner also overlooks that his copy-all-then scan configuration could pose risks of adverse impacts on the network to which a provider might object. 2d Schulzrinne Decl. ¶¶ 26-29.

Plaintiff and Mr. Bradner assert nevertheless that his conclusion is corroborated by recent U.K. Government disclosures concerning its "Section 8(4)" surveillance program. Pl.'s Opp. at 20; Bradner Decl. ¶¶ 368-69. The mere fact that the U.K. Government might be using one possible configuration does not mean that the NSA conducts Upstream surveillance in the same way, as opposed to other possible approaches. And the "rough[ ] outline" of Section 8(4) collection contained in the legal filings that Plaintiff and Mr. Bradner rely on makes it difficult to draw technical conclusions about how it compares to Upstream collection. 2d Schulzrinne Decl. ¶¶ 59-60. To the extent meaningful conclusions could be drawn from these non-technical documents, they describe, in a passage not cited by Plaintiff or Mr. Bradner, a collection approach quite comparable to the traffic-mirroring approach discussed by Dr. Schulzrinne. *Id.* ¶¶ 61-65.[5]

2. Mr. Bradner's view that a filter-then-copy-and-scan approach is "implausible" is also without a technical basis.

Mr. Bradner also gives a number of reasons why he concludes that the filter-then-copy-and-scan approach described by Dr. Schulzrinne is "implausible," Bradner Decl. ¶¶ 366-67, including several already addressed above. *See id.* ¶ 366(a), (c). But each reason given is based on assumptions about the NSA's surveillance priorities, capabilities, and targets, or simply unexplained altogether.

a. Blacklisting port or protocol numbers (HTTP and HTTPS communications): Mr. Bradner considers it implausible that the NSA would blacklist particular types of communications, specifically encrypted HTTPS communications, for several reasons. Principally, he remarks that blacklisting would leave "blind spot[s]" in the NSA's Upstream surveillance that "[s]ophisticated targets" could "easily probe" to discover and exploit to avoid surveillance. Bradner Decl. ¶ 366(b), (e). He does not explain what it is that targets could "probe," or how, to discover these so-called

[5] Wikimedia also states in its brief that Mr. Bradner's conclusions are "corroborated" by the U.S. Government's cyber-defense system known as EINSTEIN 2.0, Pl.'s Opp. at 20, although, tellingly, Mr. Bradner does not. *See* Bradner Decl. ¶ 259. As Dr. Schulzrinne explains, because the fundamental purpose and required processing capacity of EINSTEIN 2.0 differ fundamentally from those of Upstream collection, the architecture and operation of EINSTEIN 2.0 are unlikely to provide insight into Upstream's operational details. 2d Schulzrinne Decl. ¶¶ 66-70.

blind spots, *see* 2d Schulzrinne Decl. ¶ 32, what level of technical sophistication would be required, or how he presumes to know that the NSA's targets possess that level of sophistication. At bottom, whether the creation of "blind spot[s]" is a matter of such genuine intelligence concern as to dissuade the NSA from blacklisting certain types of communications depends on information concerning its mission priorities and resources known to the NSA, but not to Mr. Bradner.

Mr. Bradner also remarks that blacklisting HTTP and HTTPS communications would leave a "very large hole" in the NSA's Upstream collection, including web-based e-mail, webchat, and web-based editors, Bradner Decl. ¶ 366(f), (g), again making assumptions about the value the NSA places on particular types of communications, rather than offering a technical reason why the NSA could not or would not block access to such communications. *See* 2d Schulzrinne Decl. ¶ 34.[6]

None of the additional reasons given by Mr. Bradner for concluding that the NSA is "likely" acquiring HTTPS communications has a technical basis. That the "minimization procedures" governing Section 702 surveillance activities (which include PRISM as well as Upstream), generally authorize the NSA to collect encrypted communications (of which there are many kinds), Bradner Decl. ¶¶ 325, 366(g); *see, e.g.*, PCLOB Report at 7, does not mean that the NSA specifically acquires HTTPS communications under Upstream. The NSA's reference in a FISC filing to collection of "web activity," Bradner Decl. ¶¶ 314-15, 366(f) & n.126, is entirely consistent with targeted collection (through combined black- and whitelisting) of specific types of web activity, such as webmail or chat, but not websites such as Wikimedia's. 2d Schulzrinne Decl. ¶ 36(b). And Mr. Bradner's observations that the NSA may, now or in the future, be able to decrypt encrypted communications, Bradner Decl. ¶ 326(a), (b), or that it could learn "useful information" from the unencrypted addressing information in encrypted HTTPS communications, *id.* ¶¶ 326(c), 366(g), is

[6] He also overlooks the fact that through a combination of blacklisting and whitelisting, it is feasible to block access to all HTTP and HTTPS communications except those to or from the IP addresses of specific sites of intelligence interest (including specific chatrooms and webmail sites, to use Mr. Bradner's examples), leaving less of a hole than Mr. Bradner assumes. *See id.* ¶ 35.

merely speculation about the NSA's capabilities and priorities, not a technical basis for dismissing blacklisting of HTTPS communications as "implausible." 2d Schulzrinne Decl. ¶¶ 36(c)-38.

b. Blacklisting Wikimedia IP addresses: Next, Mr. Bradner finds it "basically inconceivable" that the NSA would blacklist Wikimedia's IP addresses, Bradner Decl. ¶ 367(a), for reasons having nothing to do with Internet engineering or technology. First he finds it "totally unbelievable" that the NSA would sift through millions of websites to decide which not to monitor. *Id.* This is again taking issue with a proposal Defendants have not made; because almost all web traffic (97 percent) is accounted for by the top 1,000 sites, eliminating unwanted volumes of communications by identifying and blacklisting certain high-volume but perhaps low-interest websites (such as, hypothetically, Wikimedia's) would be a trivial task, as Dr. Schulzrinne explains. 2d Schulzrinne Decl. ¶¶ 39-41. Second, Mr. Bradner states that blacklisting Wikimedia IP addresses would deprive the NSA of "potentially valuable" information concerning its targets' "use of Wikimedia resources," Bradner Decl. ¶ 367(a), which is again nothing more than twofold speculation about the reading habits of NSA targets and the intelligence value the NSA would ascribe to knowing whether they read certain Wikimedia websites.

c. Whitelisting IP addresses of interest: Mr. Bradner finds whitelisting implausible because in his estimation it is not possible for the NSA to know its targets' IP addresses in advance. *Id.* ¶ 366(d). He premises this conclusion, however, on unsubstantiated assumptions about the number and nature of the NSA's Upstream targets, and the NSA's intelligence capabilities.

First he assumes that the NSA has over 120,000 Upstream targets, whereas the Government report he relies on discloses only the number of Section 702 targets generally, without specifying how many of those are Upstream versus exclusively PRISM targets. *Id.*, App. Y at 14. Also, Mr. Bradner has no knowledge of the NSA's sources and methods for discovering the likely IP addresses (or address blocks) of its Upstream targets' communications, which could include communications acquired under PRISM, Executive Order 12333, Upstream collection itself, intelligence shared by

other U.S. agencies, or other sources. Second, Mr. Bradner assumes the NSA's Upstream targets include individuals (rather than other entities) who engage in movements from place to place that cause changes in their IP addresses. Bradner Decl. ¶¶ 334, 366(d).[7] In short, Mr. Bradner lacks a technological basis for dismissing whitelisting as implausible. 2d Schulzrinne Decl. ¶¶ 48, 52.[8]

3. Mr. Bradner's "certainty" that the NSA has copied and scanned at least some Wikimedia communications, even if the NSA employs traffic-mirroring techniques, lacks a non-speculative technical basis.

Finally, Mr. Bradner asserts without explanation that even if the NSA were using traffic-mirroring techniques that can filter out Wikimedia communications, it is still "virtually certain," in his estimation, that the NSA has copied and scanned at least some of Wikimedia's communications. Bradner Decl. ¶ 370. On inspection this certainty, too, is exposed as speculation.

Mr. Bradner does not dispute the *effectiveness* of blacklisting HTTP and HTTPS communications, or of whitelisting by IP address, as a means (if used) of blocking access to Wikimedia communications. Rather, of all the traffic-mirroring techniques Dr. Schulzrinne discusses, Mr. Bradner asserts only that it is "technologically incorrect that blocking [*i.e.*, blacklisting] Wikimedia's IP addresses would block all Wikimedia traffic." Bradner Decl. ¶ 367(b). Although Plaintiff repeatedly alludes in its opposition to multiple so-called "technical inaccuracies" in Dr. Schulzrinne's declaration, Pl.'s Opp. at 1, 7, 21, 24, this is the sole point of technical inaccuracy that Mr. Bradner raises with Dr. Schulzrinne's analysis. And in the end it is Plaintiff and Mr. Bradner, not Dr. Schulzrinne, who have drawn the wrong conclusion from the point Mr. Bradner raises.

---

[7] Even if that were so, such individuals' communications could be tracked using blocks of IP addresses, given their reasonable correlation with geographic areas. 2d Schulzrinne Decl. ¶ 47.

[8] Plaintiff separately argues that proposed whitelisting "ignores" (i) the NSA's collection of "about" communications that are neither to nor from its targets, and (ii) the fact that NSA selectors (such as e-mail addresses) do not appear in packet headers where addressing information (such as IP addresses) is contained. Pl.'s Opp. at 21-22. While a technical point of sorts, it is one *not* made by Mr. Bradner, and thus lacking putative support from Plaintiff's expert, it requires no response. Nevertheless, Dr. Schulzrinne explains why Plaintiff has erroneously conflated two separate steps in the filter-then-copy-and-scan process he has described. 2d Schulzrinne Decl. ¶¶ 49-52.

Mr. Bradner posits three scenarios in which Wikimedia's communications would still be copied and scanned by the NSA even if the NSA blacklisted communications containing Wikimedia IP addresses. Bradner Decl. ¶ 367(b). While each of these scenarios is theoretically possible, they could come to pass only in the uncertain event that particular conditions are met in which individuals, meeting specific criteria identified by Mr. Bradner (such as foreign individuals using U.S. e-mail services, or U.S.-based virtual private network (VPN) services), engage in communications with Wikimedia. *See id.* ¶¶ 367(b)(1)-(3). While Wikimedia claims to engage in communications with persons in almost every country on Earth, traversing every "international Internet link" with the United States, *see id* ¶ 6(d), neither Wikimedia nor Mr. Bradner cites evidence concerning the number or geographic locations of persons meeting the criteria that Mr. Bradner specifies. Thus, there is no basis to conclude that the three particular types of communications he posits cross every international Internet link to and from the United States, *or, critically*, that they cross one or more links that happen to be monitored (assuming any) by the NSA. 2d Schulzrinne Decl. ¶¶ 76-85.

Moreover, as Dr. Schulzrinne emphasizes, even if there remained a possibility of copying and scanning Wikimedia communications despite blacklisting Wikimedia IP addresses, that would not be the case if the NSA were employing a whitelisting technique. Therefore, the hypothetical possibility that Wikimedia communications could be copied and reviewed in the limited and uncertain sets of circumstances suggested by Mr. Bradner, notwithstanding blacklisting, does not alter the conclusion that the NSA, through whitelisting, could conduct Upstream surveillance without copying, scanning, or otherwise interacting with Wikimedia communications. *Id.* ¶ 86. Therefore, Mr. Bradner's assertion that the NSA "almost certainly" has copied and scanned at least some of Wikimedia's communications, even if the NSA employs traffic-mirroring techniques, Bradner Decl. ¶ 370, has no technical foundation that rises above the level of conjecture. *Id.* ¶ 87.

4. Passing remarks by the PCLOB concerning the "comprehensiveness" of Upstream's goals supply no basis on which to conclude that the NSA copies and scans Wikimedia's communications.

Finally, Plaintiff and Mr. Bradner emphasize what they call repeated Government statements that the goal of Upstream collection is to "comprehensively obtain its targets' communications." Pl.'s Opp. at 17 (quoting Bradner Decl. ¶ 335); *see id.* at 5, 8, 11, 18, 21, 23. According to Plaintiff, if the NSA's goal is to acquire all the communications of its targets, then "as a matter of technological necessity" it must be copying and scanning all communications on a monitored circuit, including Plaintiff's. *Id.* at 18.[9] But Plaintiff cannot support the case it has otherwise failed to make by resting on inchoate notions of "comprehensiveness." A similar standing argument was advanced, and rejected, in *Obama v. Klayman*, 800 F.3d 559 (D.C. Cir. 2015). The plaintiffs there asserted that the NSA must have obtained records of their phone calls, as part of its bulk phone records collection program, arguing that the "NSA's collection must be comprehensive in order for the program to be most effective." *Id.* at 567 (Williams, S.J.). The D.C. Circuit rejected this argument, observing that "there are various competing interests that may constrain the government's pursuit of effective surveillance," including "legal constraints, technical challenges, budget limitations, or other interests." *Id.*; *see id.* at 569 (Sentelle, S.J.) (agreeing with Judge Williams' views).

So too, here. As Dr. Schulzrinne explains, from the perspective of someone who has studied the economics and technology of large-scale network engineering,

> It is one thing to state these goals [of comprehensiveness], and quite another to design, construct, deploy, maintain, and pay for the collection systems required, in the numbers and with the capacity needed, to attain such ambitious goals. We cannot assume on the basis of a stated goal alone that the NSA has achieved that desired result without assuming away the technical, logistical, and financial hurdles,

[9] Notably, the "repeated" "Government" statements to which Plaintiff and Mr. Bradner refer, *see, e.g.,* Bradner Decl. ¶ 333, are actually an incidental remark by the PCLOB (not the NSA), concerning "abouts" collection, that appears twice in the PCLOB Section 702 report. The PCLOB was established for the purpose, *inter alia*, of reviewing Executive Branch counter-terrorism activities to ensure they are balanced with the need to protect privacy and civil liberties. 42 U.S.C. § 2000ee(a), (d). It is not responsible for the conduct or oversight of NSA intelligence-gathering activities, nor is it a member of the Intelligence Community, *see* 50 U.S.C. § 3003(4).

> the resource constraints and trade-offs, and the competing mission priorities, that would stand in the way.

2d Schulzrinne Decl. ¶ 73; *see* 1st Schulzrinne Decl. ¶ 74. Even assuming that the NSA has achieved a "comprehensive" level of collection, it would be possible to do so using traffic-mirroring techniques, rather than taking a copy-all-then-scan approach. 2d Schulzrinne Decl. ¶ 74. In the end, it is simply not possible to "reverse-engineer" details about Upstream's operation from so limited and technically unenlightening a starting point as abstract notions of comprehensiveness. *Id.*[10]

* * *

In sum, when attention moves beyond the pejoratives aimed at Dr. Schulzrinne's analysis – "implausible," "fanciful," "ignores key features of Upstream surveillance" – and turns to the meat of Mr. Bradner's analysis, no non-speculative basis in Internet technology or engineering can be found for questioning Dr. Schulzrinne's conclusion that Upstream surveillance could be conducted in a number of technically feasible ways that could avoid interaction with Wikimedia's communications. *See* 2d Schulzrinne Decl. ¶¶ 2, 87, 99-100. The "virtual certainty" of Mr. Bradner's opinion that the NSA is copying and scanning at least some of Wikimedia's communications sits atop "belief [and] speculation" regarding the NSA's surveillance practices and priorities, its resources and capabilities, and the number, nature, and habits of its targets, classified matters about which Mr. Bradner has no "specialized knowledge." *See Nease*, 848 F.3d at 231; *Oglesby*, 190 F.3d at 250. As a result, his opinions fail *Daubert*'s test of reliability, and are inadmissible under Rule 702.[11]

---

[10] Plaintiff also argues that the NSA could not acquire wholly domestic "about" communications at a (hypothetically) monitored international link if it were not copying and scanning all communications. Pl.'s Opp. at 22. This, too, is a technical argument not taken up by Mr. Bradner, *see* Bradner Decl. ¶¶ 293-94, and which therefore requires no response, but which Dr. Schulzrinne nevertheless explains is mistaken. 2d Schulzrinne Decl. ¶¶ 56-58.

[11] The Court need not question Mr. Bradner's stated expertise in Internet technology, *see* Bradner Decl. ¶¶ 9-18, to reach that conclusion. As other expert witnesses have done, Mr. Bradner has strayed from his field of expertise into another realm (covert NSA surveillance) about which he can offer only "subjective belief [and] unsupported speculation" rather than facts. *Zellers v. Nextech N.E., LLC*, 533 F. App'x 192, 197 (4th Cir. 2013) (testimony of expert toxicologist excluded where he lacked training in refrigerant toxicity and relevant data); *Free v. Bondo-Mar-Hyde Corp.*, 25 F. App'x

Plaintiff notes that Mr. Bradner's is the only expert testimony purporting to address the likelihood that the NSA copies and scans its communications during Upstream collection. Pl.'s Opp. at 14. That is so, because Dr. Schulzrinne focused on the issue of "technological necessity" that until now Plaintiff has insisted was the crux of this case, and refrains from engaging in the sort of uninformed speculation in which Mr. Bradner has indulged. See 2d Schulzrinne Decl. ¶¶ 2, 3. But precisely because Mr. Bradner's testimony is inadmissible, Plaintiff lacks evidence to carry its burden of proving that the NSA copies and scans its communications at the international Internet links (if any) the NSA monitors. That being so, "there can be no genuine issue as to any material fact" concerning Plaintiff's standing. *Celotex Corp. v. Catrett*, 477 U.S. 317, 322-23 (1986).

Even if Mr. Bradner's testimony somehow eked past the threshold of admissibility, it is so dependent on conjecture regarding the NSA's surveillance practices, capabilities, and targets that it would still fail, as a matter of law, to support Plaintiff's claim of standing. *See Amnesty Int'l*, 568 U.S. at 420 (standing cannot rest "on mere conjecture about possible government action"); *Defenders of Wildlife*, 504 U.S. at 560 (injury in fact must be actual or imminent, not conjectural or hypothetical). In either event the result is the same: summary judgment must be awarded to Defendants.

C. The State Secrets Privilege Would Bar Trial of Plaintiff's Standing, Even if There Were a Genuine Issue of Material Fact as to Whether the NSA Copies and Scans Plaintiff's Communications.

Defendants have shown that even if Plaintiff raised an issue of material fact, its standing could not be tried without risking or requiring harmful disclosures of privileged state secrets. Defs.' Br. at 28-30. Plaintiff makes three principal arguments in response. Pl.'s Opp. at 28-30.

First, Plaintiff contends that the Government's assertion of the state secrets privilege merely renders unavailable particular pieces of evidence, so that the case may proceed based on Plaintiff's

170, 172 (4th Cir. 2002) (testimony of "accomplished metallurgist" excluded for lack of knowledge regarding aerosol can manufacturing process); *see also Oglesby*, 190 F.3d at 250 (testimony of "qualified mechanical engineer" inadmissible where "he had no factual basis by which to reach [his] conclusion"). That misstep requires that Mr. Bradner's testimony be excluded.

presentation of unclassified materials. *See id.* at 29. Plaintiff cites (*see id.*) but one case in support of its crabbed interpretation of the state secrets privilege: *United States v. Reynolds*, 345 U.S. 1 (1953). But while in *Reynolds*, "dismissal was unnecessary because the privileged information was peripheral to the plaintiffs' action," *El-Masri*, 479 F.3d at 306, "[t]he effect of a successful interposition of the state secrets privilege by the United States will vary from case to case," *id.*[12] "Resolution of this issue will depend on the centrality of the privileged material to the claims or defenses asserted by either party." *El-Masri v. Tenet*, 437 F. Supp. 2d 530, 538–39 (E.D. Va. 2006), *aff'd* 479 F.3d 296 (4th Cir. 2007). Where "the very question on which a case turns is itself a state secret, or the circumstances make clear that sensitive military secrets will be so central to the subject matter of the litigation that any attempt to proceed will threaten disclosure of the privileged matters, dismissal is the proper remedy." *Id.* (quoting *Sterling v. Tenet*, 416 F.3d 338, 348 (4th Cir. 2005)); *see also* Defs.' Br. at 28–30.[13]

Second, according to Plaintiff, the Government does "not explain what privileged information would be placed at risk" if this case were to proceed and thus Plaintiff argues that "no harm" could come from trying, based solely on unclassified materials, whether the NSA copies and reviews Plaintiff's communications. *See* Pl.'s Opp. at 29.[14] While Defendants could only outline in their initial brief the privileged information at risk and the harms that could result from its

[12] Indeed, in *Reynolds*, the Supreme Court distinguished cases in which an assertion of the state secrets privilege would preclude further litigation. *See* 345 U.S. at 11 n.26.

[13] Plaintiff objects that the Government's assertion of the state secrets privilege focused on the "risk arising from the disclosure of specific *classified* documents," Pl.'s Opp. at 29, but, in doing so, it misapprehends the scope of the Government's privilege assertion, as well as this Court's ruling. What is protected by the Government's invocation of privilege in this matter is not only certain classified documents; rather it is the seven categories of classified *information* enumerated in this Court's Order. *See Wikimedia*, 335 F. Supp. 3d at 788.

[14] Plaintiff errs when it insists this Court "ruled that Wikimedia is entitled to show that its communications are being copied and reviewed based on . . . public evidence." Pl.'s Opp. at 28. Plaintiff lifts out of context the Court's explanation that non-classified materials, including official disclosures, may be used in a civil action under 18 U.S.C. § 1810. *See Wikimedia*, 335 F. Supp. 3d at 784–85. The Court did not previously have occasion to consider—much less decide—whether Plaintiff could use unclassified materials to try to prove privileged facts now removed from the case.

disclosure, *see* Defs.' Br. at 29, the proffered testimony of Mr. Bradner now brings the classified facts Plaintiff seeks to probe and prove into undeniable focus.

As Mr. Bradner's testimony frames the issues, resolving whether Plaintiff has standing at (a hypothetical) trial would require litigation of at least the following privileged facts:

(1) Whether it is "virtually certain" that the NSA has copied and reviewed "at least some of Wikimedia's communications," Bradner Decl. ¶ 6(e); *see Wikimedia*, 335 F. Supp. 3d at 788-89 (identities of subjects of Upstream surveillance are protected by the state secrets privilege);

(2) Whether the NSA engages in a "copy-all-then-scan" approach or whether it limits the communications subject to Upstream through whitelisting or blacklisting, *see* Bradner Decl. ¶¶ 272-273, 282-89, 366-67; *see also Wikimedia*, 335 F. Supp. 3d at 788-89 (operational details are protected by the state secrets privilege);

(3) Whether the NSA conducts Upstream surveillance at one or more international Internet links, *see* Bradner Decl. ¶¶ 222-23, 225, 332; *see also Wikimedia*, 335 F. Supp. 3d at 788 (locations of Upstream surveillance are protected by the state secrets privilege);

(4) Whether the NSA intercepts and collects HTTP and HTTPS communications, *see* Bradner Decl. ¶¶ 326-27, 366(b), 366(g); *see Wikimedia*, 335 F. Supp. 3d at 788-89 (types and categories of communications are protected by the state secrets privilege);

(5) Whether the NSA has the capability to decipher various kinds of encrypted communications, *see* Bradner Decl. ¶ 326; *see Wikimedia*, 335 F. Supp. 3d at 788-89 (NSA's cryptanalytic capabilities are protected by the state secrets privilege).

If, hypothetically, a trial were held at which Plaintiff presented public evidence on these facts, Defendants would be left with just two choices, either (1) to present evidence rebutting Plaintiff's claims, if they are in error, or (2) to remain silent in the face of Plaintiff's claims, whether right or not, to avoid more harmful disclosures of privileged facts and information about the means and methods the NSA employs in Upstream surveillance.

For example, whether Wikimedia's communications have been subject to Upstream surveillance is the pivotal factual issue that has lain at the heart of this case since its inception. If Plaintiff's conjecture is wrong, to prove so at trial Defendants would have to present highly classified documents and testimony confirming that to be the case, and, in all likelihood, reveal privileged operational details and more about Upstream along the way. The Court has already

concluded that "defendants have thoroughly documented" the risks of disclosing such information, "explaining that to reveal the fact of surveillance of an organization such as plaintiff, even considering plaintiff's voluminous online communications, would provide insight into the structure and operations of the Upstream surveillance program and in doing so, undermine the effectiveness of this intelligence method." *Wikimedia*, 335 F. Supp. 3d at 789. The fact that the ultimate factual issue underpinning Plaintiff's standing "falls squarely within the ambit of the state secrets privilege," *id.*, forecloses any further proceedings here, because, as with the plaintiff's effort to establish his alleged rendition in *El-Masri*, "the entire aim" of litigation regarding Plaintiff's standing here would be "to prove the existence of state secrets." 437 F. Supp. 2d at 539; *see also Sterling*, 416 F.3d at 348.

The situation would be no better if Defendants remained silent at trial, for that would lead to a "worst of both world[s]" scenario of the kind condemned in *Al-Haramain Islamic Found., Inc. v. Bush*, 507 F.3d 1190, 1204 (9th Cir. 2007). If Plaintiff's allegations were correct, then Defendants' silence would be tantamount to confirmation of the fact, *see id.*, "risk[ing] disclosure by implication." *See Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1089 (9th Cir. 2010). And if Plaintiff's claims were inaccurate, the Government would also be deprived of its defense as the price of invoking its privilege, an outcome expressly rejected by the Supreme Court, *see Reynolds*, 345 U.S. at 12, and by the Fourth Circuit, which "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) (first quoting *El-Masri*, 479 F.3d at 309–10; and citing *Sterling*, 416 F.3d at 347).

Similar intractable problems would arise at a trial covering other elements of Mr. Bradner's testimony. For example, relying on his testimony, Plaintiff seeks to put at issue such operational details of Upstream collection as whether the NSA filters communications using traffic-mirroring techniques, Pl.'s Opp. at 10-11, 21-24; Bradner Decl. ¶¶ 272, 280-89, 363-64, 366-67, the types and locations of the circuits it monitors, *see* Bradner Decl. ¶¶ 222-23, 225, 332, what kind of communications it acquires, *see id.* ¶¶ 326, 359, 366, and its decryption capabilities, *see id.* ¶¶ 325,

326(a)-(c). These are only several of the many components of Mr. Bradner's proffered testimony regarding the operational details of the Upstream collection process that would be squarely at issue if a trial regarding Plaintiff's standing were to proceed, and regarding which the Government could not speak without recourse to information that the Court has already found to be privileged. *Wikimedia*, 335 F. Supp. 3d at 788–89.

As a result, to hold a trial on these matters would compel Defendants either to disclose masses of privileged information about the subjects, methods, locations, scope, and capabilities of NSA surveillance in order to rebut Plaintiff's allegations; or to remain mute at trial, thus disclosing by implication the classified facts the privilege is supposed to protect (if Plaintiff's allegations are correct), or allowing the Court to proceed in error (if they are not). None of these outcomes is countenanced by the state secrets doctrine.

Finally, Plaintiff contends that a trial may proceed because, "[t]o the extent that sensitive information is implicated by future proceedings . . . FISA's procedures expressly authorize the Court to review such materials *in camera*." Pl.'s Opp. at 29–30 (citing 50 U.S.C. § 1806(f)). But the Fourth Circuit has explained that *Reynolds* "expressly foreclose[s]" such *in camera* review of information when the state secrets privilege is asserted. *El-Masri*, 479 F.3d at 311 (citing *Reynolds*, 345 U.S. at 10).[15] More to the point, this Court has already foreclosed Plaintiff's argument when it ruled that Section 1806(f)'s procedures are not available "unless a determination has previously been made that the surveillance at issue did, in fact, occur," *Wikimedia*, 335 F. Supp. 3d at 781,[16] and that, when those

[15] *See also Amnesty Int'l*, 568 U.S. at 412 n.4 (condemning *in camera* and *ex parte* judicial procedures whose very outcome would reveal targets of Government surveillance); *Abilt*, 848 F.3d at 317 (rejecting plaintiff's argument "that 'protective measures,' particularly in camera review, are adequate to protect . . . state secrets"); *El-Masri*, 437 F. Supp. 2d at 539 ("[W]here 'the whole object of the suit . . . is to establish a fact that is a state secret' . . . it is clear that the use of special procedures during . . . trial would be wholly inadequate to preserve the United States' privilege.").

[16] While Plaintiff argues that it need only establish a genuine issue of material fact as to whether its communications were subject to surveillance to invoke § 1806(f), *see* Pl.'s Opp. at 30 n.13, this Court's decision makes clear that the provision is inapplicable "where, as here, a plaintiff

procedures are applicable, they can be used only to determine the legality of surveillance, not—as Plaintiff seeks to do here—to determine whether the surveillance occurred to begin with. *See* 50 U.S.C. § 1806(f) (providing for *ex parte* and *in camera* procedures to determine if electronic surveillance was "lawfully authorized and conducted"); *Wikimedia*, 335 F. Supp. 3d at 782 (§ 1806(f) applicable where "the central dispute" is "how, and whether, information obtained via that electronic surveillance can be used or disclosed in a proceeding").

* * *

At bottom, "well-established and controlling legal principles require" that Plaintiff's private interests "must give way to the national interest in preserving state secrets," *El-Masri*, 437 F. Supp. 2d at 539, and for this reason, too, summary judgment must be awarded to Defendants.

III. THE ADDITIONAL INJURIES ASSERTED BY PLAINTIFF ARE NOT TRACEABLE TO UPSTREAM SURVEILLANCE AS A MATTER OF LAW.

Apart from the unproven claim that the NSA copies and scans its communications, Plaintiff asserts that it has also suffered two "additional injuries" that "independently establish its standing": (1) an alleged impairment of its ability to communicate with its community members, and (2) "protective measures" it allegedly has taken against "the NSA's intrusions." Pl.'s Opp. at 25-27. These claims of injury rest, at bottom, on subjective and speculative fears of surveillance, not actual surveillance of Wikimedia, and are foreclosed as a matter of law, therefore, by *Amnesty International*, 568 U.S. at 415-18 & n.7, and *Laird v. Tatum*, 408 U.S. 1, 10–16 (1972).

Plaintiff claims first that "NSA surveillance" has driven a number of its community members to "self-censor their speech or limit their engagement with Wikimedia." Pl.'s Opp. at 26. But Upstream surveillance is limited to targeting non-U.S. persons located outside the United States who are reasonably believed to possess, receive, or communicate foreign-intelligence information

---

has not yet established that it has been the subject of electronic surveillance." *Wikimedia*, 335 F. Supp. 3d at 780; *see also id.* at 782 ("Congress intended the provisions of § 1806(f) to apply where evidence already establishes the fact of surveillance."); *id.* ("Congress did not intend § 1806(f) to apply in situations where, as here, it is yet unclear whether electronic surveillance even occurred.").

approved for collection by the FISC. *See* Defs.' Br. at 2-3 (citing PCLOB Section 702 Report at 41-46). Plaintiff offers no evidence that individuals self-censored or limited their communications with Wikimedia because they were actual targets or subjects of Upstream surveillance.

To the contrary, the "public disclosures" to which Plaintiff ascribes its community members' self-censorship consist principally of unsubstantiated media hyperbole about NSA surveillance, such as headline claims that the NSA "collects nearly everything a user does on the Internet."[17] A close look at the reported "NSA slides" that Plaintiff takes as proof of NSA surveillance of its communications, *see* Pl.'s Opp. at 26, reveals that the slides do not even mention the NSA, or Upstream surveillance. *See* Pl.'s Exhs. 28, 30. Nevertheless, according to Plaintiff's declarants (whose testimony on this point is inadmissible hearsay, Fed. R. Evid. 801), these reports gave rise to fears among community members overseas that the NSA, after acquiring their communications, could identify them and perhaps disclose their communications to their home governments, which might then suppress (or retaliate against them for) their expressive activities and associations.[18] Community members also expressed fears about NSA surveillance generally, and generalized fears of "countless government agencies," including the "CIA and other intelligence-gathering organisations [sic]," and surveillance by other countries.[19]

Thus, any fears to which reports about NSA surveillance gave rise were based on "a speculative chain of possibilities," *see Amnesty Int'l*, 568 U.S. at 410-14, and attributable to the media's exaggerated and unsubstantiated portrayal of NSA intelligence-gathering activities, not to knowledge

---

[17] *See* Pl.'s Opp. at 25 & n.10; Pl.'s Exh. 27. *See also* Pl.'s Exh. 3, Decl. of Michelle Paulson ("Paulson Decl."), ¶¶ 43-48, 57-58; Pl.'s Exh. 4, Decl. of James Alexander ("Alexander Decl."), ¶¶ 4-16; Defs.' Exh. 10, Alexander Depo. 187:11-190:8; Defs.' Exh. 11, Paulson Depo. 110:18-112:2.

[18] Alexander Decl. ¶¶ 6-7, 10-11; Paulson Decl. ¶ 45 & n.8; Pl.'s Exh. 6, Decl. of Emily Temple-Wood ("Temple-Wood Decl.") ¶¶ 21-23; Defs.' Exh. 10, Alexander Depo. at 45:2-48:10, 190:10-191:6, & 74:4-91:8; Defs.' Exh. 11, Paulson Depo. at 37:5-41:12, 74:7-75:13, 112:3-113:12.

[19] Alexander Decl. ¶ 7; *see also id.* ¶ 10 (discussing community members' concern that the Philippines government "will take hard measures like spying on Filipino citizens and collaborating with the NSA"). *See also* Pl.'s Exh. 8, at WIKI0006469-70; Pl.'s Exh. 12.

of how these lawfully authorized and closely overseen programs operate, or, most pertinently, to actual NSA surveillance of Wikimedia.[20] In any event, both the press reports, and the so-called "NSA slides," are no more than unauthenticated hearsay, inadmissible as proof of any truths concerning Upstream surveillance. Fed. R. Evid. 801-802, 901(a).[21] Without such proof, any fears these reports generated in the Wikimedia community cannot be attributed to Upstream surveillance.

As further proof that Upstream surveillance impairs engagement by its community members, Plaintiff relies on the opinion of Dr. Jonathon Penney, a "legal academic and social scientist." Pl.'s Exh. 2, Decl. of Dr. Jonathan Penney ("Penney Decl.") ¶ 2, ECF No. 168-6; Pl.'s Opp. at 25-26. Dr. Penney conducted a study of total monthly page views of 48 articles posted on Wikipedia, from which he concludes that "public awareness" of NSA surveillance "is highly likely to have caused [a] sharp and sustained drop in readership" of those articles beginning in June 2013. Pl.'s Opp. at 26; Penney Decl. ¶¶ 10-11, 22-58). But before Dr. Penney's opinion can be admitted under Rule 702, it must be shown that it "rests on a reliable foundation and is relevant to the task at hand." *Zellers*, 533 F. App'x at 196 (citing *Daubert*, 509 U.S. at 588). Dr. Penney's testimony fails on both points.

Dr. Penney's opinion is irrelevant for at least two reasons. First, he fails to examine any page view data after August 2014. Thus, as explained in the declaration of statistician Dr. Alan Salzberg, even if Dr. Penney's conclusions were reliable and accurate (and they are not), his data fail to show

---

[20] Wikimedia itself may have contributed to its own community members' fears. *See* Paulson Decl. ¶ 49 (citing a July 31, 2013, Twitter post by Wikipedia co-founder Jimmy Wales, stating that the "NSA [is] snooping on what YOU are reading at Wikipedia"); *see also* Defs. Exh. 14, Jimmy Wales and Lila Tretikov, "Stop Spying on Wikimedia Users" (N.Y. Times, March 10, 2015); *see also* Defs' Exh. 15, *Wikimedia v. NSA: Wikimedia Foundation files suit against NSA to challenge upstream mass surveillance* (Mar. 10, 2015) (public announcement stating that "Using upstream surveillance, the NSA intercepts virtually all internet communications flowing across the … internet's backbone.").

[21] According to the *Guardian* articles cited by Plaintiff, the so-called slides, which purport to be classified, were obtained from Edward Snowden. But the slides' lack of authentication cannot be cured by inadmissible, multi-layered hearsay in a newspaper article. *See Gantt v. Whitaker*, 57 F. App'x 141, 150 (4th Cir. 2003) ("This circuit has consistently held that newspaper articles are inadmissible hearsay to the extent that they are introduced to prove the factual matters asserted therein."). Indeed, the lack of authentication is incurable, because as this Court has held, whether the slides are authentic or not is a state secret. *Wikimedia*, 335 F. Supp. 3d at 787-88.

that any hypothesized drop in readership of these 48 articles persisted at the time this suit was filed in March 2015, or continues today. Defs.' Exh. 7, Salzberg Decl. ¶¶ 4(H), 65, & 70; *see also id.*, ¶¶ 27-32. Dr. Penney's conclusions are therefore wholly irrelevant to the question of ongoing harm.

Second, while Dr. Penney purported to measure a hypothesized "chilling effect" of "public awareness" of NSA surveillance, he cites as the source of this "awareness" the same exaggerated and unsubstantiated press reports as does Plaintiff. *See* Penney Decl. ¶¶ 26-30. Indeed, to illustrate the "chill" he purports to measure, he quotes one Wikipedia editor as saying that "people are far less likely to engage with us, *if they know that the American government is watching their every move*." *Id.* ¶ 17 (emphasis added). Dr. Penney fails to analyze, however, whether the claimed "chilling effect" was due to genuine awareness of the true nature of the NSA's surveillance activities (much less to actual surveillance), or to exaggerated and unsubstantiated fears fomented in the press. He also fails to examine whether the claimed effect was attributable to reports about Upstream collection specifically, rather than other NSA surveillance programs, other governments' surveillance, or even other, unrelated, events occurring in June 2013. Salzberg Decl. ¶¶ 4(I), 66. His conclusions are therefore irrelevant to Upstream's claimed chilling effect on the Wikimedia community.

Dr. Penney's conclusion is also unreliable because his study does not properly "appl[y] [statistical] principles and methods." Fed. R. Evid. 702(d). As Dr. Salzberg explains, Dr. Penney's results are not reliable because his study is based on a "deeply flawed" statistical model that, *inter alia*, (i) improperly aggregates vastly different sets of page-view data, which tells a misleading story, (ii) fails to test the validity of his hypothesis that page views of the 48 articles peaked in June 2013, and (iii) ignores virtually all other factors that could have affected views of the subject articles during the period studied, including seasonal variations in readership that Wikimedia itself acknowledges. Salzberg Decl. ¶¶ 4, 47-71; *see* Alexander Depo. at 149. Penney also improperly used "comparison" datasets to validate his results that were not, in fact, comparable to the page-view data in his study. Salzberg Decl. ¶¶ 40-51. As a result of these and many other flaws, Dr. Penney's statistical model

led to spurious results that directly contradict even a simple analysis of the actual trends in the data. *Id.* ¶¶ 47, 11-26. And if the (improperly) aggregated data can be said to show anything at all, it is that the drop in page views of these 48 articles began *before* June 2013, and so could not be attributed to the June 2013 "disclosures" about NSA surveillance. *Id.* ¶¶ 18-26, 48-50.[22] Being neither reliable nor relevant, Dr. Penney's opinion is inadmissible.

Plaintiff also adduces no evidence that the "protective measures" it has taken—converting its webpages from HTTP to HTTPS-by-default, implementing Internet Security Protocol (IPSec) for certain online transmissions of proprietary data, and making changes to its staff's modes of communication, Pl.'s Opp. at 27—are attributable to actual surveillance of its communications. Rather, the evidence shows that Wikimedia's decision to implement these measures was based on its own speculative fears of surveillance, and the fears of community members, provoked in June 2013 by the same exaggerated and unsubstantiated reporting about NSA surveillance discussed above. *See* Paulson Decl. ¶¶ 49, 51, 53. [23]

Even that is a generous interpretation of the facts. The evidence also shows that Plaintiff was already considering, or had begun implementing, these measures well before the June 2013 "disclosures," as early as 2011. *See id.*; Defs.' Exh. 12, *Securing access to Wikimedia sites with HTTPS*. Plaintiff also admits that there were many other reasons to take these protective measures, having nothing to do with Upstream surveillance.[24] Particularly meritless is any suggestion that Wikimedia

[22] Indeed, Dr. Salzberg demonstrates that Dr. Penney's flawed model could equally be used to "prove" that Wikimedia's page views declined due to the Boston Marathon bombing, an event that occurred in April 2013. Salzberg Decl. ¶¶ 52–53.

[23] Plaintiff also claims as injury the new technical infrastructure it acquired and the retention of a full-time engineer, Pl.'s Opp. at 27, but these are merely incidents of implementing HTTPS-by-default and IPSec encryption. 2d Schulzrinne Decl. ¶ 94; *see* Paulson Decl. ¶¶ 54-55.

[24] Plaintiff identified a long list of such reasons, in fact, including: (i) other NSA surveillance practices; (ii) other U.S. government surveillance practices; (iii) surveillance practices of foreign state actors; (iv) practices of commercial actors; (v) individual computer hackers; (vi) responding to civil subpoenas, (vii) responding to government subpoenas; and (viii) keeping policies up-to-date and

implemented HTTPS-by-default, rather than "opt in" HTTPS (a supposedly "less burdensome" approach), due to Upstream surveillance. *See* Paulson Decl. ¶ 51. During an exchange in an online user forum in June 2015, a Wikimedia staff person explained that adopting HTTPS-by-default "[was]n't an anti-NSA measure," but "due to security and privacy concerns on a number of different levels, not all of them related to governments." Defs.' Exh. 13, Wikipedia: Village pump (technical)/Archive 138, § "HTTPS by default," at WIKI0006883; Paulson Depo. 124:19-130:5.[25]

Also conspicuously missing from the testimony proffered by Plaintiff is any suggestion that Wikimedia would abandon HTTPS-by-default, or forgo IPSec encryption of its online data transmissions, if the NSA ceased Upstream surveillance. Indeed, in today's online communications environment, there are numerous reasons why an organization such as Wikimedia, that operates major websites, and transmits large volumes of proprietary data across the Internet, would be "powerfully motivated" to retain HTTPS-by-default, and IPSec encryption, even if the NSA were not conducting Upstream surveillance. 2d Schulzrinne Decl. ¶¶ 88-98, 101. Without evidence that the so-called "injuries" of implementing HTTPS-by-default, and IPSec encryption, would be redressed by the injunctive relief Plaintiff seeks, these "injuries" cannot confer standing to sue. *See Amnesty Int'l*, 568 U.S. at 409; *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992).

In the final analysis, however, none of the additional injuries that Plaintiff asserts is traceable to Upstream surveillance, as a matter of law, and for that reason none establishes its standing. The evidence is clear that each injury claimed—the impaired engagement with community members, and the costly protective measures—is at best attributable to community members' speculative fears of Upstream surveillance, of the consequences they fear could follow, and perhaps, too, speculative

---

transparent. *See* Defs.' Exh. 9, Pl.'s Resp. & Obj. to U.S. DOJ's 1st Set of Interrogs., Resp. to Interrog. No. 16.

[25] *See also id.*, at WIKI0006885 ("While this may have been tangentially related to concerns over the NSA, it wasn't the driving force. There are other governments and private actors to take into account. . . . [I]t was driven by concern for the privacy and security of editors and readers all over the world, which means there are many different problems to consider.").

fears of surveillance among Wikimedia staff, rather than actual Upstream surveillance of Wikimedia communications to which Plaintiff can point. The Supreme Court unequivocally held in *Amnesty International* 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. 568 U.S. at 417-18 n.7 (citing *Laird*, 408 U.S. at 10-14). The Court also held that "costly and burdensome measures to protect the confidentiality of [a party's] communications" are not traceable to the Government's conduct when they are undertaken, as here, "in response to a speculative threat of surveillance." *Id.* at 415-17.

Plaintiff's efforts to side-step these holdings do not fare well. Plaintiff cites the Fourth Circuit's conclusion that its allegations of self-censored speech were sufficient to establish its standing to sue for a First Amendment violation. Pl.'s Opp. at 26. But that conclusion was predicated on the Court of Appeals' determination that Plaintiff had also plausibly alleged that its communications are copied and scanned. *Wikimedia*, 857 F.3d at 211. But now, without evidence to make good on that claim, Plaintiff is left in exactly the same position as the other, now-dismissed plaintiffs, whom the Fourth Circuit held could not establish standing based on claims of chilled speech when they had not adequately pled that the NSA intercepted their communications. *Id.* at 216 (citing *Amnesty Int'l*, 568 U.S. at 416). Plaintiff attempts to distinguish *Laird* by arguing that "unlike in *Laird*, Wikimedia challenges warrantless surveillance of private communications," Pl.'s Opp. at 26, but that was precisely the conduct challenged in *Amnesty International*, which relied for its traceability analysis on *Laird*. As Plaintiff remarks, the Court in *Amnesty International* observed that "[i]n some instances" it has found standing "based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm." Pl.'s Opp. at 27 (citing 568 U.S. at 416 n.5). But the Court concluded that the facts in *Amnesty International* did not present such an instance, because of the "attenuated chain of inferences necessary to find harm." 568 U.S. at 414 n.5. The same conclusion follows here.

IV. WIKIMEDIA DOES NOT HAVE THIRD-PARTY STANDING TO ASSERT THE CLAIMED RIGHTS OF ITS USERS.

It is unclear why Plaintiff asserts third-party standing on behalf of certain Internet users, Pl.'s Opp. at 27-28, but the effort fails. In order to "overcome the prudential limitation on third-party standing," 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." *Freilich v. Upper Chesapeake Health, Inc.*, 313 F.3d 205, 215 (4th Cir. 2002). Plaintiff satisfies none of these requirements. First, as demonstrated above, *supra*, at 4-17, Plaintiff has not shown that any of its communications have been subject to Upstream surveillance, and thus it cannot show injury in fact. The third-party standing inquiry can and should end there.

Second, Plaintiff has failed to demonstrate a "close relationship"—or indeed any relationship in any real sense—with the three categories of anonymous Internet users on whose behalf it seeks to sue. *See* Pl.'s Opp. at 27-28. Indeed, it presents no evidence that these three categories of persons even exist. Plaintiff presents no evidence, for example, that communications of "individual users inside the U.S." with Wikimedia servers abroad, or communications of "U.S. persons abroad" with U.S. Wikimedia servers, "are subject to Upstream surveillance." *Id.* Plaintiff cannot have a "close relationship" with groups of individuals whose very existence is yet to be ascertained. *Cf. Kowalski v. Tesmer*, 543 U.S. 125, 130-31 (2004) (attorneys seeking to challenge state law restricting appointment of counsel for indigent defendants did not have a "close relationship" with "as yet unascertained . . . criminal defendants"). Plaintiff claims to have a close relationship with its volunteers and contributors, Pl.'s Opp. at 28 (citing Paulson Decl. ¶¶ 8-12), but proffers no evidence that any of its volunteers and contributors fall within the three categories of Internet users it wishes to represent.

Third, Plaintiff has not shown that these three categories of Internet users face a "genuine obstacle" to bringing suit on their own behalf. *Singleton v. Wulff*, 428 U.S. 106, 116 (1976). Arguing to the contrary, Plaintiff proffers the declaration of a Wikimedia "community member" who claims

that her "workload as a medical student" makes it "impossible" for her to be a plaintiff, Temple-Wood Decl. ¶¶ 1, 26, but such "normal burdens of litigation" are insufficient. *See Am. Immigration Lawyers Ass'n v. Reno*, 199 F.3d 1352, 1364 (D.C. Cir. 2000). Ms. Temple-Wood remarks that "serving as a plaintiff in a lawsuit would threaten the anonymity [upon which Wikimedia] users depend." Pl.'s Exh. 6, Temple-Wood Decl. ¶ 27. But putative plaintiffs need not reveal as much about themselves as Ms. Temple-Wood has done, *id.* ¶ 19, to show that they are ordinary Internet users who happen to visit Wikimedia websites. Such mundane revelations do not trigger the same privacy concerns that courts have recognized as a deterrent to rightholders' defense of their own interests. *See, e.g.*, *Carey v. Population Servs., Int'l*, 431 U.S. 678, 684 n.4 (1977) (minors chilled from buying contraceptives); *Singleton*, 428 U.S. at 117 (privacy of patients seeking abortion). Plaintiff's third-party standing arguments should be rejected.

CONCLUSION

Summary judgment should be entered in favor of the Defendants.

Dated: February 15, 2019

Respectfully submitted,

JOSEPH H. HUNT
Assistant Attorney General

ANTHONY J. COPPOLINO
Deputy Branch Director

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

RODNEY PATTON
Senior Trial Counsel

JULIA A. BERMAN
Senior Counsel

OLIVIA HUSSEY SCOTT
Trial Attorney

U.S. Department of Justice Civil Division, Federal Programs Branch
1100 L Street, N.W., Room 11200
Washington, D.C. 20005

Phone: (202) 514-3358
Fax: (202) 616-8470
Email: james.gilligan@usdoj.gov

Counsel for Defendants

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

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

APPENDIX

TO

REPLY BRIEF IN SUPPORT OF DEFENDANTS' MOTION FOR SUMMARY JUDGMENT

RESPONSE TO PLAINTIFF'S STATEMENT OF MATERIAL FACTS

Defendants respond to Plaintiff's Statement of Material Facts as follows:[1]

1. Sentences one and two are undisputed for purposes of Defendants' summary judgment motion, but are not material. Sentence three is undisputed, for purposes of Defendants' summary judgment motion, to the extent it means that in 2017 Wikipedia's website received visits from more than 1 billion unique devices each month. The rest of sentence three is undisputed, for purposes of Defendants' summary judgment motion, except that the cited evidence does not support a claim that "hundreds of millions" of people "contribute" to Wikipedia.

2. Undisputed for purposes of Defendants' summary judgment motion.

3. Undisputed for purposes of Defendants' summary judgment motion.

[1] Neither the local rules of the District of Maryland nor the Eastern District of Virginia required Plaintiff, which is not moving for summary judgment, to set forth a statement of material facts. *See* L.R. 105 (D. Md.); L.R. 56(B) (E.D. Va.). As a result, Defendants are not required to respond to Plaintiff's statement of material facts, but do so nevertheless for the Court's convenience.

4. Sentence one is disputed. Upstream surveillance is limited to targeting non-U.S. persons located outside the United States who are reasonably believed to possess, receive, or communicate foreign-intelligence information approved for collection by the FISC. *See* PCLOB Report at 5–6, 20–24, 41-46. Sentence two can neither be confirmed nor denied because the number and nature of Upstream targets are classified facts protected by the state secrets privilege. *Wikimedia Found. v. NSA*, 335 F. Supp. 3d 772, 789-90 (D. Md. 2018). Defendant's do not dispute sentence three for purposes of Defendants' summary judgment motion, to the extent that pages 103 and 116 of the PCLOB Report discuss the possibility that communications of U.S. persons may be acquired by the government as a result of incidental or inadvertent collection. *See* PCLOB Report at 103, 116.

5. Undisputed, for purposes of Defendants' summary judgment motion, to the extent that Defendants have officially acknowledged the existence of, and certain details about, the NSA's Upstream surveillance program.

6. Disputed to the extent Plaintiff's description of Upstream surveillance is inconsistent with the unclassified description set forth by the Director of National Intelligence, *see* ECF No. 138-2, Declaration of Daniel Coats ¶ 15. For example, Plaintiff describes the program as intercepting communications traversing certain "circuits" (plural), whereas whether the NSA conducts Upstream surveillance at more than one Internet backbone circuit is a classified fact protected by the state secrets privilege. *See* Coats Decl. ¶ 18; *Wikimedia Found.*, 335 F. Supp. 3d at 789-90.

7. Undisputed, for purposes of Defendants' summary judgment motion, that in 2017 the estimated number of the Government's targets (non-U.S.-persons, groups, or entities) under Section 702 of the Foreign Intelligence Surveillance Act ("FISA") exceeded 129,000. ODNI,

Statistical Transparency Report for Calendar Year 2017 (April 2018) (Pl.'s Exh. 20). Otherwise the assertions in this paragraph are disputed as unsupported by the cited exhibit.

8. The operational details of Upstream surveillance are protected by the state secrets privilege and cannot be confirmed or denied. *Wikimedia Found*, 335 F. Supp. 3d at 788-90. Defendants do not dispute, for purposes of their summary judgment motion, that during the Upstream collection process a body of at least one-end-foreign Internet transactions transiting the Internet backbone are screened for the purpose of identifying those containing at least one tasked selector. *See* Pl.'s Exh. 18, Objections and Responses by Defendants National Security Agency and Adm. Michael S. Rogers, Director, To Plaintiff's Interrogatories, Response To Interrogatory No. 9.

9. The first sentence is undisputed to the extent that Upstream results in transactions containing selectors being ingested into NSA systems, *see* Coats Decl. ¶ 15, and to the extent the term "long-term retention" is consistent with unminimized Internet transactions being aged off of the NSA systems no later than two years after the expiration of the Section 702 certification under which the data has been acquired. *See* PCLOB Section 702 Report at 60. The second and third sentences are undisputed, for purposes of Defendants' summary judgment motion, to the extent that, prior to April 2017, Upstream surveillance involved "about" collection and now it does not.

10. The scope and scale of Upstream surveillance are facts protected by the state secrets privilege and cannot be confirmed or denied. *See* Coats Decl. ¶ 18; *Wikimedia Found.*, 335 F. Supp. 3d at 788-90. As to the second sentence, Defendants do not dispute that the PCLOB Section 702 Report, at 143, states that "[t]he success of [the Upstream collection] process depends on collection devices that can reliably acquire data packets associated with the proper communications."

11. The types communications acquired through Upstream surveillance are facts protected by the states secrets privilege and cannot be confirmed or denied. *Wikimedia Found.*, 335 F. Supp. 3d at 788-90. Also disputed inasmuch as the term "web activity" used in the cited

document may have been intended to refer to Internet activity as a whole, for reasons including, *inter alia*, that it is common in colloquial usage to use the term "web" when referring to the Internet at large. *See* 2d Schulzrinne Decl. ¶ 36(b).

12. Defendants can neither confirm nor deny whether Upstream surveillance occurs at one or more "international Internet links," nor whether it occurs at more than one circuit on the Internet backbone, because those facts are protected by the state secrets privilege, *see* Coats Decl. ¶ 18; *Wikimedia Found.*, 335 F. Supp. 3d at 789-90; it is undisputed, for purposes of Defendants' summary judgment motion, that Upstream collection occurs at one or more locations that are "upstream" in the flow of communications between communication service providers. *See* PCLOB Section 702 Report at 35. Disputed to the extent Plaintiff relies on inadmissible hearsay to support this fact. *See* Defs.' Reply at 4-6.

13. The first sentence is disputed to the extent Plaintiff's description of Upstream surveillance is inconsistent with the unclassified description set forth by the Director of National Intelligence, *see* ECF No. 138-2, Declaration of Daniel Coats ¶ 15. Defendants do not dispute, for the purposes of Defendants' summary judgment motion, that the Internet backbone (which is no longer well defined) may be understood for the purposes of Defendants' summary judgment motion as the principal high-speed, ultra-high bandwidth data-transmission lines between the large, strategically interconnected computer networks and core routers that exchange Internet traffic domestically with smaller regional networks, and internationally via terrestrial or undersea circuits. See Pl.'s Ex. 18, NSA Response to Interrog. 12. Regarding the remaining portions of paragraph 13, the operational details of Upstream surveillance, including the locations at which it is conducted, whether it occurs at one or more "international Internet links," and whether it occurs at more than one circuit on the Internet backbone, are facts protected by the state secrets privilege and cannot be confirmed or denied. *See* Coats Decl. ¶ 18; *Wikimedia Found.*, 335 F. Supp. 3d at 788-90.

14. Undisputed, for purposes of Defendants' summary judgment motion.

15. Defendants do not dispute, for purposes of Defendants' summary judgment motion, that it is "virtually certain" that Wikimedia communications traverse every international cable connecting the U.S. to other countries. Defendants can neither confirm nor deny whether the NSA monitors "international Internet links" in the course of conducting Upstream surveillance because that is a fact protected by the state secrets privilege. *See* Coats Decl. ¶ 18; *Wikimedia Found.*, 335 F. Supp. 3d at 789-90.

16. The first sentence is not disputed for purposes of Defendants' summary judgment motion. The second sentence is disputed to the extent Plaintiff's description of Upstream surveillance is inconsistent with the unclassified description set forth by the Director of National Intelligence, *see* ECF No. 138-2, Declaration of Daniel Coats ¶ 15. The remaining operational details of Upstream surveillance are protected by the state secrets privilege and cannot be confirmed or denied. *See* Coats Decl. ¶ 18; *Wikimedia Found.*, 335 F. Supp. 3d at 788-90.

17. The operational details of Upstream surveillance are protected by the state secrets privilege and cannot be confirmed or denied. *See* Coats Decl. ¶ 18; *Wikimedia Found.*, 335 F. Supp. 3d at 788-90. Also, disputed on the ground that the assertions contained in paragraph 17 are unsupported by reliable expert testimony based on Internet technology and engineering. *See generally* 2d Schulzrinne Decl.

18. The operational details of Upstream surveillance are protected by the state secrets privilege and cannot be confirmed or denied. *See* Coats Decl. ¶ 18; *Wikimedia Found.*, 335 F. Supp. 3d at 788-90. Also, disputed on the ground that the assertions contained in paragraph 18 are unsupported by reliable expert testimony based on Internet technology and engineering. *See generally* 2d Schulzrinne Decl.

19. The operational details of Upstream surveillance, including the number of the NSA's Upstream targets, are facts protected by the state secrets privilege and cannot be confirmed or denied. *See* Coats Decl. ¶ 18; *Wikimedia Found.*, 335 F. Supp. 3d 788-90. Also, disputed on the ground that the assertions contained in paragraph 19 are unsupported by reliable expert testimony based on Internet technology and engineering. *See generally* 2d Schulzrinne Decl.

20. The assertions in paragraph 20 are argumentative and as such require no response. To the extent a response is required, Defendants state that the operational details of Upstream surveillance are facts protected by the state secrets privilege and cannot be confirmed or denied. *See* Coats Decl. ¶ 18; *Wikimedia Found.*, 335 F. Supp. 3d 788-90. Also, disputed on the ground that the assertions contained in paragraph 20 are unsupported by reliable expert testimony based on Internet technology and engineering. *See generally* 2d Schulzrinne Decl.

21. Not material. *See* 2d Schulzrinne Decl. ¶¶ 59-64. The Court is respectfully referred to the cited document for a complete and accurate statement of its contents.

22. The operational details of Upstream surveillance are facts protected by the state secrets privilege and cannot be confirmed or denied. *See* Coats Decl. ¶ 18; *Wikimedia Found.*, 335 F. Supp. 3d at 788-90. Also, disputed on the ground that the assertions contained in paragraph 22 are unsupported by reliable expert testimony based on Internet technology and engineering. *See generally* 2d Schulzrinne Decl.

23. The operational details of Upstream surveillance—including the nature and number of its targets, the location(s) of the surveillance, and whether it occurs at more than one circuit—are facts protected by the state secrets privilege and cannot be confirmed or denied. *See* Coats Decl. ¶ 18; *Wikimedia Found.*, 335 F. Supp. 3d at 788-90. Also, sentence three is disputed on the ground that the assertions contained in paragraph 23 are unsupported by reliable expert testimony based on Internet technology and engineering. *See generally* 2d Schulzrinne Decl.

24. Defendants can neither confirm nor deny whether Plaintiff has been subject to Upstream surveillance because that is a classified fact subject to the state secrets privilege. *See* Coats Decl. ¶ 18; *Wikimedia Found.*, 335 F. Supp. 3d at 788-90. Also, this paragraph is disputed on the ground that it is unsupported by reliable expert testimony based on Internet technology and engineering. *See generally* 2d Schulzrinne Decl.

25. Defendants can neither confirm nor deny whether Plaintiff has been subject to Upstream surveillance because that is a classified fact subject to the state secrets privilege. *See* Coats Decl. ¶ 18; *Wikimedia Found.*, 335 F. Supp. 3d at 788-90. Dispute the assertion that any public disclosures occurred concerning NSA surveillance of Wikimedia's communications, on the ground that it is unsupported by evidence, admissible or otherwise. Disputed that there was "grave concern within the Wikimedia community" to the extent Plaintiff relies on inadmissible hearsay contained within the cited declarations as support for this fact. Also, to the extent that the "public disclosures" identified in paragraph 25 are the claims made on the face of the inadmissible and unauthenticated press reports referred to within the cited declarations in paragraph 25, Defendants do not dispute that those hyperbolic and unsupported press reports may have "caused grave concern within the Wikimedia community." *See* Defs.' Reply at 23-24.

26. The assertion in sentence one concerning a "drop in readership of certain Wikipedia pages" is disputed on the ground that it is unsupported by relevant or reliable or expert testimony. *See generally* Saltzberg Decl. Also disputed that the asserted "drop in readership" (if any), "impaired … interactions," and "costly measures" were attributable to actual NSA surveillance of Wikimedia, rather than subjective and speculative fears of surveillance. *See* Defs.' Reply at 22-28.

27. Paragraph 27 contains legal conclusions to which no response is required. Also disputed on the ground that Plaintiff has presented no evidence that the editors and contributors

with whom it asserts a close relationship fall within any of the three categories of Internet users whose legal rights Plaintiff seeks to assert. *See* Defs.' Reply at 29-30.

Dated: February 15, 2019

Respectfully submitted,

JOSEPH H. HUNT
Assistant Attorney General

ANTHONY J. COPPOLINO
Deputy Branch Director

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

RODNEY PATTON
Senior Trial Counsel

JULIA A. BERMAN
Senior Counsel

OLIVIA HUSSEY SCOTT
Trial Attorney

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

Counsel for Defendants