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

DEFENDANTS' MEMORANDUM OF POINTS AND AUTHORITIES IN OPPOSITION TO PLAINTIFF'S MOTION TO COMPEL DISCOVERY RESPONSES AND DEPOSITION TESTIMONY

Dated: April 27, 2018

CHAD A. READLER
Acting Assistant Attorney General

ANTHONY J. COPPOLINO
Deputy Branch Director

JAMES J. GILLIGAN
Special Litigation Counsel

RODNEY PATTION
Senior Trial Counsel

JULIA A. BERMAN
TIMOTHY A. JOHNSON
OLIVIA HUSSEY-SCOTT
Trial Attorneys
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave., N.W., Room 6102
Washington, D.C. 20001
Phone: (202) 514-3358
Fax: (202) 616-8470
Email: james.gilligan@usdoj.gov

Counsel for Defendants

TABLE OF CONTENTS

INTRODUCTION 1

BACKGROUND 3

ARGUMENT 8

I. The State Secrets Privilege Bars Plaintiff's Discovery. 8

A. The Information Described in the DNI's Declaration and the Classified NSA Declaration is Protected by the State Secrets Privilege 8

B. Plaintiff's Contention that Releasing the Information It Seeks Would Not Harm National Security Is Entitled to No Weight, and Is Meritless 11

II. Plaintiff's Discovery Is Also Barred by the Statutory Privileges Under 50 U.S.C. §§ 3024(i)(1) and 3605(a). 14

A. The Information Plaintiff Seeks Is Protected by 50 U.S.C. § 3024(i)(1) 14

B. The Information Plaintiff Seeks Is Also Protected by 50 U.S.C. § 3605(a) 16

III. The Government's Privileges Are Not Superseded by FISA 18

A. Section 1806(f) Does Not Apply to the Instant Dispute 19

B. Section 1806(f) Does Not Displace the Government's Privileges. 24

1. To displace the state secrets privilege would require a clear and unequivocal statement of legislative intent 24

2. Neither the text nor even the legislative history of § 1806(f) contains a clear and unequivocal statement of intent to abrogate the state secrets privilege, or speaks at all, directly or otherwise, to the issue 26

3. Plaintiff's position is unsupported by other authority. 28

4. Proceeding as Plaintiff advocates would endanger national security in exactly the manner condemned by the Supreme Court in *Amnesty International*. 31

IV. Additional Grounds Requiring That Plaintiff's Motion To Compel Be Denied. 32

A. Lack of Relevance 32

B. Undue Burden 33

C. Improper Use of Requests for Admissions as Discovery Devices 35

CONCLUSION 35

INTRODUCTION

At the September 22, 2017, status conference Plaintiff Wikimedia Foundation ("Wikimedia") advised the Court that it did not need discovery to establish its standing, but nevertheless, to "bolster" its demonstration of standing, it anticipated seeking "limited discovery" from the Government in order to pose "certain clarifying questions . . . about the operation of [U]pstream [surveillance]." Tr. of Status Conf. (Sept. 22, 2017) (Exh. A.) at 14, 19-20, 23-24, 28. Thereafter, Plaintiff's understanding of the term "limited discovery" manifested itself in the form of 84 separate interrogatories, requests for admission, and document requests each served on all three Government agency Defendants in this case.

The Government responded to Plaintiff's discovery requests, and produced over 500 pages of documents, so far as it could do so without revealing classified information. To the extent, however, that Plaintiff's requests called for disclosures of classified sources and methods and operational details of Upstream surveillance, the Government objected on grounds of the state secrets privilege, and the statutory privileges established under 50 U.S.C. §§ 3024(i)(1) and 3605(a). The Government also objected, as appropriate, on grounds including lack of relevance, undue burden, and the improper use of requests for admissions as discovery devices. Dissatisfied with the Government's responses, Plaintiff has now moved to compel the National Security Agency ("NSA") and the other Government agency Defendants to disclose highly sensitive and classified information concerning Upstream surveillance in response to more than 50 of its discovery requests. *See* Pl.'s Mot. at 8-9. That motion should be denied.

The Director of National Intelligence ("DNI"), as head of the U.S. Intelligence Community, has formally invoked the state secrets privilege, and the DNI's statutory privilege under § 3024(i)(1), against disclosure of the classified information, concerning Upstream surveillance, that Plaintiff seeks. Public Declaration of Daniel R. Coats, Director of National

Intelligence (filed herewith) ("Coats Decl.") (Exh. B). The DNI's assertion of privilege is supported by the Deputy Director of the NSA, who in a classified *ex parte, in camera* declaration filed this date ("Classified NSA Decl.") explain in a level of detail that cannot be shared on the public record why disclosure of the information subject to the DNI's assertions of privilege reasonably could be expected to cause exceptionally grave damage to the national security of the United States. In addition, the Deputy Director asserts the NSA's privilege under 50 U.S.C. § 3605(a) over the same documents and information. As a result of the DNI's and the NSA's assertions of privilege, the classified information concerning Upstream surveillance that Plaintiff seeks is removed from the case entirely, and Plaintiff's motion to compel must fail.

Plaintiff's principal argument to the contrary is that a provision of the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1806(f), preempts all of the Government's privileges invoked here, including the state secrets privilege. But, by its terms § 1806(f) does not apply here. In proceedings where the Government seeks to use surveillance-based evidence against a target or subject of that surveillance, § 1806(f) provides a mechanism for *ex parte* review of materials related to the surveillance, for the purpose of determining its legality. It does not allow litigants such as Plaintiff to discover whether they have been targets or subjects of surveillance in the first place. Indeed, whereas Congress intended § 1806(f) as a mechanism allowing the Government to protect sensitive sources and methods of surveillance, applying it in these circumstances, for the purposes envisioned by Plaintiff, would turn it into a weapon to compel disclosures of sensitive sources and methods over the Government's objection.

Nor does the legislative history or precedent support Plaintiff's interpretation. Taken as a whole, the statutory text and the statements of Congress and the courts regarding § 1806(f) demonstrate that it has no application here, and does not affect—much less displace—the state secrets privilege or the related statutory privileges the Government has asserted in this case.

For these and all the reasons discussed below, Plaintiff's motion to compel disclosure of classified sources, methods, and operational details of Upstream surveillance should be denied.

BACKGROUND

Plaintiff seeks to contest the legality of Upstream surveillance, under which the NSA targets non-U.S. persons, located abroad, to obtain foreign-intelligence information. Using its Upstream collection capabilities, the NSA acquires targeted communications that transit the Internet "backbone" networks of U.S. telecommunications service providers. Upstream surveillance is conducted under authority of Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1881a, pursuant to targeting and minimization procedures approved by the Foreign Intelligence Surveillance Court (the "FISC"). *See id.* § 1881a(c)(1)(A). Plaintiff nevertheless maintains that Upstream collection exceeds the Government's authority under Section 702, violates the Constitution, and should be enjoined. At issue in these proceedings is whether Plaintiff has Article III standing to assert these claims.

Plaintiff's Standing Allegations

Although the technical operational details of Upstream surveillance remain classified, Plaintiff alleges that it involves an initial stage at which NSA devices intercept and copy a substantial number of the international online communications (including Plaintiff's) transiting the U.S. telecommunications network, and scan them in-transit to identify communications containing selectors associated with the NSA's surveillance targets. Am. Compl. (ECF No. 70-1) ¶¶ 47, 49, 50. Plaintiff alleges that targeted communications, once identified, are ingested into Government databases and retained for analysis and may be disseminated. *Id.* ¶ 49.

In support of the assertion that the NSA copies and scans at least some of its online communications, Plaintiff alleges that the "sheer volume" and global distribution of its communications, together with the assumption that the NSA "must be" copying and reviewing

all communications that travel across any point on the Internet backbone that it monitors, make it "virtually certain" that the NSA intercepts at least some of these communications. *Id.* ¶¶ 57-65.

Prior Proceedings

In October 2015, the Court granted the Government's motion to dismiss the claims of Wikimedia and its erstwhile co-plaintiffs, holding they had not adequately pled their standing. *Wikimedia Found. v. NSA*, 143 F. Supp. 3d 344 (D. Md. 2015). On appeal, the Fourth Circuit agreed that Wikimedia's co-plaintiffs had not plausibly alleged their standing, but concluded otherwise in Wikimedia's case, based on three "key" allegations: (1) that, given their great volume and worldwide distribution, Plaintiff's "communications almost certainly traverse every international backbone link connecting the United States with the rest of the world"; (2) that, due to alleged "technical rules of how the Internet works," the NSA "must be copying and reviewing all the international text-based communications that travel across a given link" where it conducts Upstream surveillance; and (3) that the NSA is conducting surveillance on "at least one" Internet backbone link. *Wikimedia Found. v. NSA*, 857 F.3d 193, 210-11 (4th Cir. 2017).

Plaintiff's Discovery Requests[1]

On remand, the Court authorized five months' time (later extended to six) for discovery limited to the issue of jurisdiction. ECF Nos. 117, 123. As noted above, Plaintiff served a total of 84 separate discovery requests on the Government, more than 50 of which are at issue in its motion to compel, divided into three categories. *See* Pl.'s Mot. at 8-9. The first category Plaintiff describes as seeking "direct evidence" that it "has been surveilled" in the course of Upstream surveillance. *See* Pl.'s Mot. at 3-4 (discussing Pl.'s Request for Admission ("RFA") Nos. 16-21; 34-36; Pl.'s Request for Production of Documents ("RFP") Nos. 23-24. To protect

[1] Plaintiff's discovery requests, as well as Defendants' responses and objections thereto, may be found at Exhibits 2 through 19 to the Declaration of Patrick Toomey, ECF No. 125-3.

classified information whose disclosure would risk exceptionally grave damage to national security, the Government has refused to confirm or deny, or to produce documents indicating, whether Wikimedia communications have been subject to Upstream surveillance.

The second category of information at issue in Plaintiff's motion to compel is designated as "[k]ey terms used in describing Upstream surveillance to the public." Pl.'s Mot. at 4. This category includes responses to Plaintiff's Interrogatory Nos. 1-9, which ask the Government to describe its understanding of the "definitions" of terms and phrases used in various public documents to discuss the Upstream surveillance process in general and unclassified terms. While the Government set forth its understanding of most of these terms and phrases, so far as it was possible to explain them without revealing classified information about Upstream surveillance, *see* ECF No. 125-14, NSA Resp. to Pl.'s Interrogatory Nos. 1-9,[2] the Government objected to these requests for "definitions" to the extent they sought classified information about the sources and methods and technical operational details of Upstream surveillance.

The third and largest category of requests to which Plaintiff seeks to compel responses is labeled in its motion as "Evidence concerning the scope and breadth of Upstream surveillance." Pl.'s Mot. at 6. This wide-ranging category includes discovery requests seeking information and documents to show, *inter alia*, the number, nature, and type of point(s) on the Internet backbone where Upstream surveillance is conducted, *see* Interrogatory Nos. 16-17, RFA Nos. 13-15, 16, 25-30, 39, RFP Nos. 14-15; the volume of Internet communications traffic subject to various stages of Upstream surveillance, *see* Interrogatory Nos. 18-19, RFP No. 10; the type(s) of communications subject to such surveillance, *see* RFA Nos. 37-38; the manner in which the NSA

[2] The Government was unable, however, to provide any response to Interrogatory Nos. 1 and 7, which sought the Government's understanding of the terms "international Internet link," as used by the FISC in an October 3, 2011, memorandum opinion, and of the common technical characteristics of so-called Internet "packets" comprising an "Internet transaction."

conducts Upstream surveillance, *see* RFA Nos. 6-10; the NSA's decryption capabilities, *see* Interrogatory No. 20; RFA 40; and, lest any stone go unturned, the entire process by which any communications are "interacted with" during the Upstream process, *see* Interrogatory No 14.

While the Government was able to respond, at least in unclassified part, to some of these requests,[3] by and large the Government had to object to them so as to protect classified information in the interest of national security. In addition, the Government objected on grounds of undue burden to RFP No. 10, seeking documents sufficient to show the number of Internet communications acquired through Upstream surveillance over an eight-year period, which arguably called for the production of entire databases of communications acquired by the NSA.

Plaintiff's motion to compel also includes in both its second and third categories all documents responsive to RFP Nos. 21 and 22, *see* Pl.'s Mot. at 8-9, which seek all FISC, Foreign Intelligence Surveillance Court of Review ("FISC-R"), and Supreme Court opinions and orders concerning Upstream surveillance, and all submissions to these courts concerning Upstream surveillance, since the enactment of Section 702 in July 2008.[4] As set forth in a separate declaration by the Office of the Director of National Intelligence ("ODNI"), the documents responsive to RFP Nos. 21 and 22, all of which contain classified information, exceed 10,000 pages in length. Declaration of Lauren L. Bernick (filed herewith) ("Bernick Decl.") (Exh. C) ¶¶ 7, 8. The Government objected to producing any documents in response to

[3] For example, the Government was able to respond, at least in unclassified part, to Plaintiff's RFA Nos. 6, 8, and 10, which inquire about the manner in which communications are reviewed during the Upstream collection process. Similarly, in response to Plaintiff's RFP No. 10, the NSA produced arguably responsive documents regarding the number of communications acquired through Upstream surveillance during the first six months of 2011. The Government also directed Plaintiff to public websites where it had posted (in unclassified form) the NSA's Section 702 Targeting Procedures for the years 2016 and 2017 in response to RFP No. 18.

[4] Neither the FISC-R nor Supreme Court has issued any opinions or orders concerning Upstream, nor has the Government made filings concerning Upstream in either court.

these requests, because of their classified nature, and the enormous burden of producing over 10,000 pages of classified documents in unclassified (*i.e.*, redacted) form. *See id.* ¶¶ 8-13.[5]

The DNI's and the NSA's Assertions of Privilege

To prevent disclosures of classified information concerning sources, methods and operational details of Upstream surveillance that reasonably could be expected to cause exceptionally grave damage to national security, the DNI has asserted the states secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1), over the information sought by Plaintiff's motion to compel. *See* Coats Decl. ¶¶ 7, 9, 12, 16, 17, 48. In his *in camera, ex parte* declaration, the Deputy Director of the NSA explains in classified detail the basis for the DNI's assertions of privilege, and asserts the statutory privilege under 50 U.S.C. § 3605(a) over the same information. While Plaintiff divides the information it seeks into three categories, to understand the exceptionally grave risk to national security that would flow from its disclosure, it is best viewed as falling into the seven distinct categories identified below. The DNI's and NSA's assertions of privilege encompass information in each category, whether responsive to Plaintiff's pending discovery requests, to future discovery Plaintiff may seek, or that may otherwise be necessary to litigate Plaintiff's claims or the Government's defenses.

These seven categories are enumerated at greater length in both the Classified NSA Declaration and the DNI's declaration, but they may be summarized thus: (A) Entities subject to Upstream surveillance activities, *see* RFA Nos. 16-21, 34-36; RFP Nos. 21-24; (B) Operational

[5] In addition to the foregoing requests, Plaintiff has indicated it will file a supplemental motion to compel further testimony from an NSA official who was deposed on April 16, 2018, pursuant to Federal Rule of Civil Procedure 30(b)(6). Pl.'s Mot. at 10-11; Pl.'s Supp. to Its Mot. to Compel (ECF No. 136) at 3. The designated NSA witness was questioned for nearly seven hours on the record on topics concerning Upstream surveillance that were largely coextensive with the subjects of Plaintiff's written requests. Because Plaintiff's questions consistently called for classified information about the sources and methods and operational details of Upstream surveillance, it was necessary throughout the deposition for the NSA to withhold information in response. The Government will respond to Plaintiff's supplemental motion when filed.

details of the Upstream collection process, *see* Interrogatory Nos. 3-5, 14, 15; RFA Nos. 6-10, 37, 38; RFP Nos. 21, 22; (C) Location(s) on the Internet backbone at which Upstream surveillance is conducted, *see* Interrogatory Nos. 1, 2; RFA Nos. 13-15, 25-30, 39; RFP Nos. 13, 15, 16, 18, 21, 22; (D) Categories of Internet-based communications subject to Upstream surveillance activities, *see* Interrogatory Nos. 6-8; RFA Nos. 16-18; RFP No. 22; (E) the scope and scale on which Upstream surveillance is or has been conducted, *see* Interrogatory Nos. 9, 16-19; RFP Nos. 10, 14; (F) NSA decryption capabilities, *see* Interrogatory No. 20; RFA No. 40; and (G) Additional categories of classified information contained in opinions and orders issued by, and in submissions made to, the FISC, *see* RFP Nos. 21, 22. *See* Coats Decl. ¶ 18.

ARGUMENT

I. THE STATE SECRETS PRIVILEGE BARS PLAINTIFF'S DISCOVERY.

The privilege for military and state secrets to protect information vital to the national security "is well established." *United States v. Reynolds*, 345 U.S. 1, 6-7 (1953). The state secrets privilege has a constitutional foundation in the President's Article II powers to conduct foreign affairs and provide for the national defense. *See United States v. Nixon*, 418 U.S. 683, 710 (1974); *Abilt v. CIA*, 848 F.3d 303, 312 (4th Cir. 2017) ("The state secrets privilege performs a function of constitutional significance, because it allows the executive branch to protect information whose secrecy is necessary to its [national security] responsibilities."). The state secrets privilege is absolute, and "even the most compelling necessity cannot overcome" it. *Reynolds*, 345 U.S. at 11; *Sterling v. Tenet*, 416 F.3d 338, 343 (4th Cir. 2005).

A. The Information Described in the DNI's Declaration and the Classified NSA Declaration Is Protected by the State Secrets Privilege.

To ensure that the privilege is asserted only when necessary, the Government must satisfy three procedural requirements to invoke the state secrets privilege: (1) there must be a "formal claim of privilege;" (2) the claim must be "lodged by the head of the department which has

control over the matter;" and (3) the claim must be made "after actual personal consideration by that officer." *See Reynolds*, 345 U.S. at 7-8. All three requirements are satisfied here: the DNI, the head of the U.S. Intelligence Community, has formally asserted the privilege after personally considering the matter and determining that the disclosures of information Plaintiff seeks to compel reasonably could be expected to cause serious damage, and in many cases exceptionally grave damage, to national security. Coats Decl. ¶¶ 16, 24, 28, 32, 35, 39, 43.

Once the privilege has been properly invoked, a court "must determine whether the information that the United States seeks to shield is a state secret, and thus privileged from disclosure." *El-Masri v. United States*, 479 F.3d 296, 304 (4th Cir. 2007). A privilege assertion must be sustained if the court is satisfied, "from all the circumstances of the case, that there is a reasonable danger that compulsion of the evidence will expose . . . matters which, in the interest of national security, should not be divulged." *Reynolds*, 345 U.S. at 10; *Abilt*, 848 F.3d at 312.

"In assessing [that] risk . . . a court is obliged to accord the utmost deference" to the informed judgments of Executive Branch officials. *El-Masri*, 479 F.3d at 305. As the Supreme Court has stressed, "what may seem trivial to the uninformed, may [be] of great moment to one who has a broad view of the scene and may put the questioned item of information in its proper context." *CIA v. Sims*, 471 U.S. 159, 178 (1985); *accord Halperin v. CIA*, 629 F.2d 144, 150 (D.C. Cir. 1980) ("[E]ach individual piece of intelligence information . . . may aid in piecing together other bits of information even when the individual piece is not of obvious importance in itself."). "Frequently, the explanation of the department head who has lodged the formal privilege claim, provided in an affidavit or personal declaration, is sufficient to carry the Executive's burden" of demonstrating that the information is privileged. *Abilt*, 848 F.3d at 312.

Here, the Government has submitted both (i) a public declaration by the DNI making a formal claim of privilege and explaining the serious damage, and in some cases exceptionally

grave damage, that the disclosures of information Plaintiff seeks to compel could be expected to cause to national security; and (ii) a classified declaration from the Deputy Director of the NSA, describing this information and the harm its disclosure could cause in greater detail than is possible on the public record without revealing the very information that the DNI's assertion of privilege is meant to protect. *See generally* Coats Decl.; Classified NSA Decl.

Broadly speaking, disclosure of this information reasonably could be expected, among other things, to seriously compromise—if not entirely undermine—vital ongoing intelligence operations (in particular, Upstream collection); deprive the NSA of valuable intelligence-gathering methods, tools, and facilities needed to conduct Upstream surveillance and otherwise carry out its signals intelligence mission; and enhance the abilities of foreign adversaries both to evade NSA surveillance and to conduct their own surveillance operations against the United States and its allies. *See, e.g.*, Coats Decl., ¶¶ 23, 27, 31, 34, 38, 42. By interfering with the NSA's ability to protect the United States against foreign threats, disclosure of this information could thus reasonably be expected to cause damage, and in some cases exceptionally grave damage, to national security. *See id.* at ¶¶ 24, 28, 32, 35, 39, 43.

For such reasons, courts uniformly have held that information of the kind encompassed by the DNI's assertion of privilege, including who is and is not a subject of surveillance, and the operational details of surveillance programs, are protected by the state secrets privilege. *See, e.g.*, *Al-Haramain Islamic Found., Inc. v. Bush*, 507 F.3d 1190, 1203-04 (9th Cir. 2007) (information regarding whether plaintiff "has been subject to NSA surveillance" held a privileged state secret); *Halkin v. Helms*, 598 F.2d 1, 9 (D.C. 1978) (upholding privilege assertion over "the identity of particular individuals whose communications have been acquired"); *see also Abilt*, 838 F.3d at 314 ("sources and methods used by the CIA"); *Sterling*, 416 F.3d at 346 (intelligence-gathering methods and capabilities). Indeed, one district court has expressly found that information tending

to reveal operational details of Upstream collection is protected by the state secrets privilege. *Jewel v. NSA*, 2015 WL 545925, at *5 (N.D. Cal. Feb. 10, 2015) (finding "[d]isclosure of this classified information would risk informing adversaries of the specific nature and operational details of the Upstream collection process").

Therefore, as described more fully in the DNI's public declaration and the Classified NSA Declaration, the public disclosure of any of the information over which the DNI has asserted the state secrets privilege reasonably could be expected to cause serious damage, and in many cases exceptionally grave damage, to national security. The Government thus has demonstrated a sufficient, indeed compelling, basis for asserting the state secrets privilege in this case.

B. Plaintiff's Contention that Releasing the Information It Seeks Would Not Harm National Security Is Entitled to No Weight, and Is Meritless.

Plaintiff contends that the state secrets privilege does not apply here because the disclosures it seeks "would not harm national security." Pl.'s Mot. at 20. Plaintiff offers no valid reason to doubt the DNI's assessment of the harm likely to flow from disclosing the classified information it desires, a judgment entitled to "utmost deference." *El-Masri*, 479 F.3d at 305.

Plaintiff first argues that its online communications are so ubiquitous that revealing whether they have been subject to Upstream surveillance would disclose nothing an adversary could use to evade detection. *Id.* at 21. The Classified NSA Declaration explains, however, the numerous ways in which the requested disclosure could reveal significant information about the targets and operational details of Upstream surveillance, details that could threaten the effectiveness of NSA surveillance—all contrary to Plaintiff's necessarily uninformed arguments. *See Halkin I*, 598 F.2d at 8 (rejecting plaintiff's argument "that admission or denial of the fact of acquisition of [certain] communications" would not harm national security as "naïve").[6]

[6] In light of its large Internet presence, Plaintiff argues that disclosing that at least one of its communications has been subject to Upstream surveillance would reveal no more about NSA

Plaintiff next argues that releasing classified information about Upstream surveillance could not harm national security given "the government's extensive public disclosures concerning the operation of Upstream surveillance." Pl.'s Mot. at 22. But the premise of this argument lacks foundation. The Government, in an effort to be as transparent as possible about the NSA's intelligence-gathering activities consistent with national security, has declassified certain general facts about Upstream surveillance, but has continued to safeguard the details of its nature and operation—the very details Plaintiff seeks to find out. *See, e.g.*, Coats Decl. ¶ 15.

Moreover, the purportedly "extensive" disclosures to which Plaintiff adverts amount to bits and pieces of information contained in four documents: a report by the Privacy and Civil Liberties Oversight Board, an October 2011 FISC opinion concerning Upstream collection, a June 2011 Government submission to the FISC, and unsourced statements in a legal treatise—only one of which, the Government's submission to the FISC, was actually made by or on behalf of intelligence agencies responsible for the conduct of Upstream surveillance. *See* Pl.'s Mot. at 6-7, 22-23. Neither these documents nor any other public disclosures about Upstream surveillance have disclosed technical details of the kind Plaintiff now seeks (a fact made obvious by Plaintiff's 84 discovery requests). Rather, the Government's public disclosures about Upstream surveillance remain quite limited, and Plaintiff is trying to use the tools of discovery to pry loose additional details about Upstream surveillance that are not available in the public domain.

Furthermore, litigants seeking to compel disclosure of national security information on the basis that it already lies in the public domain must show that the information has been

---

surveillance than "confirming that an NYPD officer saw a yellow taxi cab while patrolling the streets of New York." Pl.'s Mot. at 21. That analogy reflects a fundamental misunderstanding of the clandestine manner in which the NSA must carry out its signals-intelligence mission. The NSA is more aptly viewed as an undercover officer, and confirming that it saw a yellow taxi cab would reveal to targets of its investigations that they should avoid the streets of New York, and seek to advance their illegal schemes by taking the subway instead, where no undercover officers may be present.

"officially acknowledged." *Fitzgibbon v. CIA*, 911 F.2d 755, 765 (D.C. Cir. 1990) (decision under the Freedom of Information Act ("FOIA")).[7] For an item of intelligence information to be deemed "officially acknowledged," three criteria must be satisfied. *Fitzgibbon*, 911 F.2d at 765. "First, the information requested must be as specific as the information previously released." *Id.*; *Public Citizen*, 11 F.3d at 203; *Salisbury v. U.S.*, 690 F.2d 966, 971 (D.C. Cir. 1982). "Second, [it] must match the information previously disclosed." *Fitzgibbon*, 911 F.2d at 765; *see Halkin*, 598 F.2d at 9 (disclosure that one person's communications had been monitored did not prevent the Government withholding identities of others whose communications were acquired).

These first two criteria reflect the reality that information differing in its specificity or particulars from that which already lies in the public domain can provide "additional information" to the nation's adversaries "that would be harmful to national security." *Edmonds*, 323 F. Supp. 2d at 77; *see Fitzgibbon*, 911 F.2d at 766. That is obviously the case here: for example, general disclosures about the nature of Upstream surveillance may not give foreign adversaries sufficient information about it to evade its reach, whereas specific details about its methods of operation, the location(s) at which it takes place, the types of communications targeted, and so forth, likely would. Coats Decl. ¶¶ 26-27, 30-31.

Hence, it is firmly established that the Government, having concluded in one case that disclosing intelligence information is permissible (or even advisable) in the national interest, is not prevented from concluding in another situation that a similar disclosure "may lead to an unacceptable risk" of harm to national security. *Sims*, 471 U.S. at 180-81; *see also Stein v. Dep't of Justice*, 662 F.2d 1245, 1258-59 (7th Cir. 1981).

[7] Courts have found case law under the FOIA "instructive" in ascertaining "whether a matter claimed to implicate national security is publicly known." *Terkel v. AT&T Corp.*, 441 F. Supp. 2d 899, 914-16 & n.9 (N.D. Ill. 2009) (citing *ACLU v. Brown*, 609 F.2d 277, 280 (7th Cir. 1979)).

Third, to be considered "officially acknowledged" information residing in the public domain, the specific information that is sought "must already have been made public through an official and documented disclosure" by authorized Government officials. *Fitzgibbon,* 911 F.2d at 765. Without "pointing to specific information" about Upstream surveillance "that duplicates [the information] being withheld," *Public Citizen*, 11 F.3d at 201, and which has previously been acknowledged "in an official and documented disclosure," *Fitzgibbon,* 911 F.2d at 765, Plaintiff cannot show that the information about Upstream surveillance it seeks has, in fact, been disclosed. And Plaintiff plainly cannot do that here: the general overview of Upstream surveillance that has been officially disclosed does not approach in detail the revelations about Upstream collection that Plaintiff has moved to compel. Plaintiff cites prior public disclosures about "circuits," "transactions," "screen[ing]," "scan[ning]," and "filtering" communications, Pl.'s Mot. at 22-23, but these disclosures do not begin to rival the level of specificity with which Plaintiff would have this Court force the Government to respond to its discovery requests.

In sum, Plaintiff has not shown that the Government has previously disclosed the information it seeks to protect here. Plaintiff has otherwise made no showing that would undermine the DNI's assertion of privilege, or his conclusion, and the NSA's, that public disclosure of this information reasonably could be expected to cause serious damage, in some instances exceptionally grave damage, to national security.

II. PLAINTIFF'S DISCOVERY IS ALSO BARRED BY THE STATUTORY PRIVILEGES UNDER 50 U.S.C. §§ 3024(i)(1) AND 3605(a).

A. The Information Plaintiff Seeks Is Protected by 50 U.S.C. § 3024(i)(1)

Plaintiff's motion to compel should also be denied because the discovery Plaintiff seeks is also barred by the DNI's statutory privilege under 50 U.S.C. § 3024(i)(1). Section 3024(i)(1) provides that the "[DNI] shall protect intelligence sources and methods from unauthorized disclosure." The DNI has done so here, invoking the statute to protect from unauthorized

disclosure specific sources and methods of Upstream surveillance. Coats Decl. ¶¶ 17. The seven categories of information encompassed by the DNI's assertion of privilege, concerning targets and subjects of surveillance, and the technical operational details and location(s) of Upstream surveillance, all fall within the statute's purview. Plaintiff's motion, accordingly, cannot succeed. "It is well recognized that a privilege may be created by statute," *Baldrige v. Shapiro*, 455 U.S. 345, 360 (1982), and "[i]f a privilege exists, information may be withheld, even if relevant to the lawsuit and essential to the establishment of plaintiff's claim," *id.*

Arguing to the contrary, Plaintiff asserts that Section 3024(i)(1) "has nothing to do with discovery" and "is simply not a litigation privilege." Pl.'s Mot. at 23-24. But Plaintiff is wrong. Section 3024(i)(1) is the successor statute to 50 U.S.C. § 403(d)(3), a provision that conferred on the Director of Central Intelligence ("DCI") the same authority to "protect intelligence sources and methods from unauthorized disclosure" now entrusted to the DNI. When Congress restructured the Intelligence Community ("IC"), and created the ODNI, *see* 50 U.S.C. § 3023(b)(1), Congress imbued the DNI with the same duties and responsibilities, and authority, previously conferred on the DCI. *See* Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (Dec. 17, 2004), §§ 1011-1020.[8]

Prior to these amendments, a number of courts expressly recognized the DCI's authority to protect intelligence sources and methods under Section 403(d)(3) as a litigation privilege applicable in civil discovery. *See, e.g.*, *Linder v. Dep't of Defense*, 133 F.3d 17, 25 (D.C. Cir. 1998) (acknowledging civil discovery privilege under 50 U.S.C. § 403-3(c)(5)) (formerly

[8] *See also* Senate Agreement to the Conf. Rep. on S. 2845, 150 Cong. Rec. S11939, S11965 (Dec. 8, 2004) ("The bill properly affords the DNI authority to protect intelligence sources and methods, but this is the same authority that is currently vested in the [DCI]"); House Agreement to H. Res. 870 and the Conf. Rep. on S. 2845, 150 Cong. Rec. H10994, H11004 (Dec. 7, 2004) ("The bill vests the DNI with the authority to protect intelligence sources and methods, just as the [DCI] has exercised").

codified at 50 U.S.C. § 403(d)(3)); *see also, e.g.*, *Kronisch v. United States*, 1995 WL 303625, at *1, 9 (S.D.N.Y. 1994); *United States v. Koreh*, 144 F.R.D. 218, 222 (D.N.J. 1992) ("there can be little doubt" that § 403(d)(3) "provides the basis for a statutorily based claim of privilege" against civil discovery); *Heine v. Raus*, 261 F. Supp. 570, 577-78 (D. Md. 1966), *vacated and remanded on other grounds*, 399 F.2d 785 (4th Cir. 1968).

The application of this statutory privilege to the instant case is reinforced by the Supreme Court's discussion of § 403(d)(3) in *C.I.A. v. Sims*, 471 U.S. 159 (1985). There the Court said of § 403(d)(3) that "[t]he statutory mandate . . . is clear: Congress gave the [DCI] wide-ranging authority to protec[t] intelligence sources and methods from unauthorized disclosure." *Id*. at 177. Sources and methods, the Court observed further, are "the heart of all intelligence operations," *id.* at 167, and "[i]t is the responsibility of the [DCI], not that of the judiciary, to weigh the variety of complex and subtle factors in determining whether disclosure of information may lead to an unacceptable risk of compromising the . . . intelligence-gathering process." *Id.* at 180. The DNI, as successor to that same grant of authority, has determined that disclosure of the information sought here would lead to unacceptable risks of exceptionally grave damage to national security; in the face of that determination, Plaintiff's motion to compel must fail.

B. The Information Plaintiff Seeks Is Also Protected by 50 U.S.C. § 3605(a).

Plaintiff's wide-ranging requests for information concerning the sources and methods and operational details of NSA Upstream surveillance are also barred by NSA's statutory privilege under Section 6 of the National Security Agency Act of 1959, 50 U.S.C. § 3605(a) (formerly 50 U.S.C. 402, note), which provides:

> [N]othing in this chapter or any other law . . . shall be construed to require the disclosure of the organization or any function of the National Security Agency, or any information with respect to the activities thereof, or of the names, titles, salaries, or number of the persons employed by such agency.

Id. In addition to supporting the DNI's assertions of privilege, the NSA Deputy Director, in his classified *ex parte, in camera,* declaration, asserts the NSA's statutory privilege over the same categories of information concerning Upstream collection. The statute's reach, which expressly includes information about "any function" or "activities" of the NSA, clearly extends to Upstream surveillance, and the result once again is that Plaintiff's motion to compel must be denied. "The protection afforded by Section 6 is, by its very terms, absolute. If a document is covered by Section 6, NSA is entitled to withhold it . . ." *Linder v. NSA*, 94 F.3d 693, 698 (D.C. Cir. 1996); *accord Houghton v. NSA*, 378 Fed. Appx. 235, 238-239 (3d Cir. 2010); *Roman v. NSA*, 2009 WL 303686, at *5-6 (E.D.N.Y. 2009), *aff'd* 354 Fed. Appx. 591 (2d Cir. 2009).

Plaintiff argues that Section 6 "does not have the broad meaning" the Government ascribes to it, but is revealed by its legislative history as "a statute narrowly aimed at protecting NSA's personnel records." Pl.'s Mot. at 26. Plaintiff once again is incorrect. The text of Section 6 leaves no room to doubt that it extends its protection to the "function[s] of the [NSA]" and "information with respect to [its] activities," in addition to the protection afforded to information about NSA personnel. 50 U.S.C. § 3605(a). "[W]hen [a] statute's language is plain, the sole function of the courts . . . is to enforce it according to its terms," *Lamie v. United States Tr.*, 540 U.S. 526, 534 (2004), and there is no occasion for "resort to legislative history" to discover a different meaning, *United States v. Gonzales*, 520 U.S. 1, 6 (1997).

Moreover, the D.C. Circuit has repeatedly considered and rejected Plaintiff's argument that Section 6 is limited to personnel records. *Linder*, 94 F.3d at 696; *Founding Church of Scientology v. NSA*, 610 F.2d 824, 827-28 (D.C. Cir. 1979);[9] *Hayden v. NSA*, 608 F.2d 1381,

[9] *Founding Church of Scientology*, after examining the legislative history, held that "[s]ection 6 *ordains unequivocally that 'nothing in this Act or any other law* (including, but not limited to, the [Classification Act]) shall be construed to require. . . disclosure." 610 F.2d at 828 (emphasis added).

1390 (D.C. Cir. 1979).[10] As held in *Linder*, "arguments based on [Section 6's] legislative history are trumped by the plain language of the statute. . . ." 94 F.3d. at 696. "Whatever concerns Congress may have had with the disclosure of personnel information . . . it chose statutory language that cannot be confined to so narrow a purpose; and the explicit reference to 'any other law' (which surely includes laws governing civil discovery) must be construed to prohibit the disclosure of information relating to NSA's functions and activities as well as its personnel." *Id.*

Plaintiff also cites to *dicta* in *Terkel v. AT&T Corp.*, 441 F. Supp. 2d 899, 905 (N.D. Ill. 2006), and *Founding Church of Scientology*, 610 F.2d at 828-29, expressing concern that the terms of Section 6 should not be read too broadly. Pl.'s Mot. at 26-27. Notably, in neither of these cases did the courts require disclosures of information concerning intelligence activities, over which the NSA had invoked the protection of Section 6. And here, the Court "need not grapple with" the outer bounds of Section 6's protections because the NSA's assertion of privilege in this instance is well within its established parameters. *See People for the Am. Way Found. v. NSA*, 462 F. Supp. 2d 21, 31 (D.D.C. 2006).

Because Plaintiff seeks to compel disclosure of information concerning NSA intelligence-gathering activities, namely Upstream surveillance, that falls within the well-established bounds of Section 6, and because the protection afforded by Section 6 is absolute, the Court should deny Plaintiff's motion to compel.

III. THE GOVERNMENT'S PRIVILEGES ARE NOT SUPERSEDED BY FISA.

Plaintiff argues that its motion to compel disclosures of classified information about Upstream surveillance is "govern[ed]" not by the state secrets privilege, or the Government's statutory privileges, but by a provision of FISA codified at 50 U.S.C. § 1806(f). Pl.'s Mot. at 12.

[10] *Hayden* compared Section 6 with a similar statute applicable to the CIA and, after examining the legislative history, found that "Congress certainly had rational grounds to enact for the NSA a protective statute broader than the CIA's," given Congress's determination that "disclosure of NSA activities is potentially harmful." 608 F.2d at 1390.

According to Plaintiff, § 1806(f) "displaces" the Government's privileges, and requires it instead to submit the classified documents and information at issue to the Court, which must then review these materials *in camera* and *ex parte* to determine the legality of the challenged surveillance. *Id.* at 13. In other words, Plaintiff construes § 1806(f) as requiring the Court to conduct an *in camera* review of the over 10,000 pages of documents called for by RFP Nos. 21 and 22 alone, and of entire electronic repositories of communications acquired by the NSA, *see* NSA Resps. to RFP No. 10, among other materials, in order to resolve the instant dispute.

Section 1806(f) imposes no such requirements. Section 1806(f), by its terms, does not even apply to the circumstances at bar. No matter how many times Plaintiff may say otherwise, it is not FISA's "discovery provision"—that is a term of Plaintiff's invention—but a mechanism for determining the legality of surveillance in proceedings where "aggrieved persons" contest the Government's use of surveillance-based evidence against them.[11] In any event, neither the text nor legislative history of § 1806(f) contains the clear and unequivocal statement of legislative intent that would be necessary to displace a privilege, like the state secrets privilege, whose roots lie in the Constitution's mandate to the Executive to provide for the nation's security.

A. Section 1806(f) Does Not Apply to the Instant Dispute.

Section 1806(f) lies within a provision of FISA that governs the "[u]se of information" obtained from electronic surveillance conducted under FISA, *see* 50 U.S.C. § 1806, and provides, in pertinent part:

> Whenever a court . . . [1] is notified pursuant to subsection (c) or (d) of this section, or [2] whenever a motion is made pursuant to subsection (e) of this section, or [3] whenever any motion or request is made *by an aggrieved person* pursuant to any other statute or rule of the United States . . . to discover or obtain applications or

[11] It is worth noting that the Government has never been required under this so-called "discovery provision" to produce classified information to an opposing party or its counsel. The only order by a district court requiring such disclosure was overturned on appeal. *See U.S. v. Daoud*, 2014 WL 321384, at *3 (N.D. Ill.), *rev'd*, 755 F.3d 479, 481-85 (7th Cir. 2015).

> orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter, the [court] shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary *to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted*.

Id. § 1806(f) (emphasis added). Thus, § 1806(f) authorizes procedures for the *in camera, ex parte* review of materials relating to electronic surveillance in three circumstances involving "aggrieved persons":

> (1) when the Government provides notice that it "intends to enter into evidence or otherwise use or disclose" surveillance-based evidence in proceedings against an aggrieved person (*see* 50 U.S.C. § 1806(c), (d));
>
> (2) when an "aggrieved person" moves in such a proceeding to suppress "evidence [or information] obtained or derived from an electronic surveillance" (*see id.*, § 1806(e), (f)); or
>
> (3) when an "aggrieved person" moves pursuant to any other statute or rule to "discover or obtain" "applications, order, or other materials relating to electronic surveillance" or "evidence or information obtained or derived from electronic surveillance" (*see id.* § 1806(f)).

When one of the foregoing circumstances exists, and § 1806(f) is invoked by the Attorney General through an affidavit indicating that disclosing the information sought (or an adversary hearing) would be harmful to national security, the district court is then required to review *in camera* and *ex parte* materials related to the surveillance as may be necessary "to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted." *Id.*[12] Thus, § 1806(f) does not apply here, for at least two reasons.

[12] As the Court explained § 1806(f)'s mechanism in *United States v. Rosen*, 447 F. Supp. 2d 538 (E.D. Va. 2006) (Ellis, J.), under § 1806(c), if "the government intends to use or disclose FISA evidence at the trial of an 'aggrieved person,'" the government must provide notice, upon which "an aggrieved person may seek to suppress [such] evidence" pursuant to § 1806(e). *Id.* at 545. In that event, upon attestation by the Attorney General that "disclosure of such material would harm national security, the district court must review the FISA warrant applications and related materials *in camera* and *ex parte* to determine whether the surveillance or search 'of the aggrieved person was lawfully authorized and conducted.'" *Id.* (quoting 50 U.S.C. § 1806(f)).

First, the purpose for which § 1806(f) authorizes *ex parte, in camera* review of evidence is "to determine whether . . . surveillance of [an] aggrieved person was lawfully authorized and conducted." Yet the purpose for which Plaintiff sought the classified documents and information that it now argues must be reviewed by this Court is to discover whether, for purposes of demonstrating standing, Plaintiff's communications have been subject to Upstream surveillance. Indeed, the sole issue before the Court at this stage of the case is whether Plaintiff can establish its standing to challenge Upstream surveillance, not its lawfulness. Section 1806(f) does not authorize, much less require, *ex parte, in camera* review to determine a person's *standing* to contest allegedly unlawful surveillance. The sole stated purpose of review under § 1806(f) is to ascertain whether surveillance to which it is already known the movant was subject was lawfully authorized and conducted. *See* S. Rep. No. 95-701 at 63 (explaining that the purpose of § 1806(f)'s procedure is "to determine whether the surveillance was authorized and conducted in a manner which did not violate any constitutional or statutory right of the person against whom the evidence sought is to be introduced").

Second, and relatedly, Plaintiff has not established that it is an "aggrieved person" entitled to invoke § 1806(f)'s procedures. FISA defines an "aggrieved" person as one "who is the target of . . . or whose communications or activities were subject to electronic surveillance." 50 U.S.C. § 1801(k). Because the sole determination a court may make under § 1806(f) is whether the challenged surveillance was lawfully authorized and conducted, the movant's status as an "aggrieved person" who was a subject of surveillance is an antecedent question that must be determined as a pre-requisite to, and not by means of, *ex parte* proceedings under the statute.

That conclusion also follows from the fact that each specified circumstance in which § 1806(f) applies is premised on prior Government acknowledgment that the movant has been a subject of surveillance. Notice of intended use of surveillance-based evidence under § 1806(c)

and (d) necessarily discloses the fact of surveillance. A motion to suppress such evidence under § 1806(e) occurs only after the fact of surveillance of the movant has been established. *See Rosen*, 447 F. Supp. 2d at 545. Likewise, under the established interpretive canons of *noscitur a sociis* and *ejusdem generis*, the final situation to which § 1806(f) applies—a motion to "discover or obtain" information about challenged surveillance (such as Plaintiff purports to bring here)—must also be limited to situations in which the Government has acknowledged the fact that the movant is an aggrieved person who was a subject of the surveillance. *See Washington Dep't of Soc. & Health Servs. v. Estate of Keffeler*, 537 U.S. 371, 384-85 (2003) (general terms following specific terms in a statutory enumeration are considered to embrace only matters similar to those enumerated by the preceding specific terms).[13]

Accordingly courts, including this one, have construed the term "aggrieved person" to mean that only litigants who can establish that their communications were subject to electronic surveillance may proceed under § 1806(f). *See, e.g.*, *U.S. v. Damrah*, 412 F.3d 618, 623-24 (6th Cir. 2005) (§ 1806(f) applied where Government used tapes of FISA surveillance during trial); *U.S. v. Johnson*, 952 F.2d 565, 571 & n.4 (1st Cir. 1992) (same); *Rosen*, 447 F. Supp. 2d at 545-53; *see also In re Mot. for Release of Court Records*, 526 F. Supp. 2d 484, 487 (F.I.S.C. 2007) (holding that § 1806(f) has no application outside of ensuring aggrieved persons the opportunity to contest the legality of FISA-derived evidence to be used against them). In contrast, litigants who cannot establish that they are aggrieved persons cannot invoke § 1806(f) to discover whether they are aggrieved persons in the first place, as Plaintiff seeks to do here. *See, e.g.*,

[13] That understanding of § 1806(f) is firmly supported by the legislative history. As explained in the House report accompanying FISA, § 1806(f) "sets out special judicial procedures to be followed *when the Government concedes that it intends to use or has used evidence obtained or derived from* electronic surveillance." H.R. Rep. No. 95-1283, at 90 (1978) (emphasis added). It "deals with those rare situations in which the Government states it will use evidence obtained or derived from electronic surveillance." *Id.*

ACLU Found. of S. Cal. v. Barr, 952 F.2d 457, 462, 468-69 & n.13 (D.C. Cir. 1991) (plaintiff may not use § 1806(f) to discover suspected ongoing surveillance).[14]

Plaintiff argues that it meets the definition of "aggrieved person" because the Fourth Circuit concluded that Plaintiff has plausibly alleged that at least some of its communications have been subjected to Upstream collection processes. Pl.'s Mot. at 12 (citing *Wikimedia*, 857 F.3d at 209, 211). But mere allegations are of no avail to a would-be movant under § 1806(f). Plaintiff is endeavoring now to prove that it is an aggrieved person whose communications were subject to the surveillance it seeks to contest, a purpose that falls outside the scope of § 1806(f)'s permitted application. *See Barr*, 952 F.2d at 462, 468-69 & n.13.

In short, § 1806(f) may be invoked only for the purpose of determining the legality of contested surveillance in a proceeding where FISA-based evidence may be used against an aggrieved person, and not to determine the standing of a litigant such as Plaintiff to challenge allegedly unlawful surveillance. The statute's procedures are also unavailable to litigants, such as Plaintiff, whose status as "aggrieved persons" subjected to electronic surveillance is not established beforehand. Therefore, if there were any situation in which § 1806(f) could be said to displace the state secrets privilege, or the Government's statutory privileges under § 3024(i)(1) and § 3605(a), that situation is not presented by this case.

[14] Section 1806(f) stands in contrast to 18 U.S.C. § 3504, which upon a threshold showing by a "party aggrieved" that evidence to be used against him in a proceeding is the product of unlawful surveillance, requires the Government to affirm or deny the existence of surveillance. Congress was mindful of § 3504 when it enacted FISA, but chose not to include such a requirement in § 1806. *See* S. Rep. No. 95-701 at 63 (§ 1806(f) proceedings may arise after "a defendant queries the Government under [§ 3504] and discovers that he has been [surveilled]."). One court applied § 3504's standard to § 1806(f) to conclude that merely alleging one is an aggrieved party is sufficient to trigger § 1806(f). *See In re NSA Telecomms. Records Litig.*, 700 F. Supp. 2d 1182, 1190, 1194 (N.D. Cal. 2010), *vacated on other grounds*, 705 F.3d 845 (9th Cir. 2012). For the reasons discussed herein, that decision was mistaken.

B. Section 1806(f) Does Not Displace the Government's Privileges.

Even if § 1806(f) applied here, nothing in the text or even the legislative history of the statute exhibits the clear and unequivocal statement of Congressional intent that would be necessary to "displace," preempt, or supersede the Government's invocation of the state secrets privilege. *See* Pl.'s Mot. at 13-20. For this reason as well, Plaintiff's argument that § 1806(f) "governs" its motion to compel is without merit.

1. To displace the state secrets privilege would require a clear and unequivocal statement of legislative intent.

For several reasons, Congress would need to speak clearly in a statute to override the state secrets privilege. First, "[a]lthough the state secrets privilege was developed at common law, it 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." *El-Masri*, 479 F.3d at 303. "[T]he Executive's constitutional mandate [thus] encompasses the authority to protect national security information . . . [and] to the extent an executive claim of privilege relates to the effective discharge of a President's powers, it is constitutionally based." *Id.* at 304. "The state secrets privilege . . . thus has a firm foundation in the Constitution, in addition to its basis in the common law of evidence." *Id*

A clear expression of intent is therefore required before a court can conclude that Congress meant to abrogate the Executive's authority to invoke the state secrets privilege in support of its national security functions. *See Franklin v. Massachusetts*, 505 U.S. 788, 800-01 (1992); *United States. v. Bass*, 404 U.S. 336, 349 (1971); *Armstrong v. Bush*, 924 F.2d 282, 289 (D.C. Cir. 1991). Indeed, a statute susceptible of a reading that would curtail Executive authority to protect the secrecy of information in the interest of national security would raise serious constitutional concerns, and should be construed to avoid that result unless "plainly contrary to the intent of Congress." *Public Citizen v. DOJ*, 491 U.S. 440, 465-66 (1989).

Moreover, as explained in *Reynolds*, the Executive's prerogative to withhold sensitive national security information in litigation is an attribute of sovereign immunity, not abrogated by a general waiver of immunity from suit. 345 U.S. at 6 (failure to uphold assertion of state secrets privilege "subjected the United States to judgment on terms to which Congress did not consent"). A waiver of sovereign immunity may be found only where Congress has "unequivocally expressed" that waiver "in statutory text." *FAA v. Cooper*, 566 U.S. 284, 290 (2012).

Ignoring these principles, Plaintiff relies on cases holding that a rule of "federal common law" may be "abrogate[d]" by a statute that "speak[s] directly to the question addressed by the common law." Pl.'s Mot. at 13-14 (citations omitted). But these cases address only the displacement of judge-made doctrines adopted to "fill in statutory interstices" in the absence of guidance from Congress, *see Am. Elec. Power Co. v. Connecticut.*, 564 U.S. 410, 421 (2011),[15] not a privilege grounded in authority conferred on the Executive by the Constitution itself.

Even assuming *arguendo* that the standard applied in *Texas*, *City of Milwaukee*, and *County of Oneida* applied here, Plaintiff disregards the fact that, where "a long-established and familiar" common law doctrine is at issue, statutes must be read "with a presumption favoring the retention of long-established and familiar principles, except when a statutory purpose to the contrary is evident." *Texas*, 507 U.S. at 534. The fact that a statute addresses the same subject-matter as a common-law doctrine is insufficient to displace the common-law rule. Rather, "the relevant inquiry is whether the statute 'speaks *directly* to the question' otherwise answered by federal common law," as "federal common law is used as a 'necessary expedient' when Congress has not spoken to a *particular* issue." *County of Oneida*, 470 U.S. at 236-37; *see also*

[15] *See also U.S. v. Texas*, 507 U.S. 529, 534 (1993) (common law rule that, according to *Royal Indem. Co. v. U.S.*, 313 U.S. 289, 296 (1941), developed based on the courts' "own criteria"); *City of Milwaukee v. Illinois & Michigan*, 451 U.S. 307-08, 313-14 (1981) (common law cause of action for abatement of nuisance); *County of Oneida v. Oneida Indian Nation*, 470 U.S. 226, 237 (1985) (common law remedies for unlawful conveyance of Indian land).

City of Milwaukee, 451 U.S. at 313-14 (federal statute must "speak directly" to the "particular issue" to supplant the common law.).

Regardless, however, of the standard applied, § 1806(f) does not displace the state secrets privilege.

2. Neither the text nor even the legislative history of § 1806(f) contains a clear and unequivocal statement of intent to abrogate the state secrets privilege, or speaks at all, directly or otherwise, to the issue.

Nothing in the text or even the legislative history of § 1806(f) refers to the state secrets privilege at all, much less to displacing, abrogating, or preempting the privilege. That alone should end the matter. Nevertheless, in support of its displacement theory Plaintiff argues that § 1806(f) "speaks directly to the procedures applicable to the discovery Wikimedia seeks." Pl.'s Mot. at 14. But as just shown, § III.A, *supra*, § 1806(f) is directed at a fundamentally different set of circumstances than those presented here: to determine the lawfulness of surveillance in proceedings where surveillance-derived evidence may be used against an acknowledged target or subject. Nothing in the text of § 1806(f) or its legislative history suggests that it can be invoked by parties in Plaintiff's shoes to discover in the first instance whether they have been subject to alleged unlawful surveillance. Plaintiff's displacement theory thus collapses at the outset.

Plaintiff argues that the third circumstance to which the statute applies, "whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States . . . to discover . . . materials relating to electronic surveillance," as evidence of its "universal[ ]" application. Pl.'s Mot. at 14. Plaintiff misconstrues this provision. As discussed *supra*, at 22, this clause, like those preceding it, is also narrowly limited to proceedings in which acknowledged targets or subjects of surveillance against whom surveillance-based evidence may be used seek a determination of the surveillance's legality. Plaintiff points, in addition, to language stipulating that the procedures established under § 1806(f), when applicable, must be

followed "notwithstanding any other law." *Id.* But that clause does not itself expand the statute's scope beyond what its other terms provide for.

Plaintiff also misunderstands the legislative history that it selectively quotes in its brief. *See id.* (citing S. Rep. No. 95-604, pt. 1, at 57). The legislative history shows that Congress included a catchall provision for motions filed "pursuant to any other statute or rule," and mandated application of § 1806(f)'s procedures "notwithstanding any other law," to prevent opposing parties from evading the statute's *ex parte* review mechanism, which Congress established for the protection of sensitive national security information. *See* S. Rep. No. 95-701 at 58-59 (noting that "broad rights of access" to surveillance materials "can threaten the secrecy necessary to effective intelligence practices"); *see also id* at 63-64; H.R. Conf. Rep. No. 95-1720 at 32. The purpose was not to compel the Government to disclose privileged information over its objection, *see id.* at 65, the misguided interpretation that Plaintiffs seek to impose on the statute's terms. As explained by the Senate Judiciary Committee:

> Although a number of different procedures might be used to attack the legality of the surveillance, it is this procedure "notwithstanding any other law" that must be used to resolve the question. The Committee wishes to make very clear that the procedures set out in[§ 1806(f)] apply whatever the underlying rule or statute referred to in the motion. *This is necessary to prevent the carefully drawn procedures in [§ 1806(f)] from being bypassed by the inventive litigant using a new statute, rule or judicial construction.*

S. Rep. No. 95-604, pt. 1, at 57 (emphasis added). *See also* S. Rep. No. 95-701, at 63 (1978) (same); H.R. Rep. No. 95-1283, at 91 (same).

Plaintiff again resorts without avail to the legislative history when it observes that Congress enacted FISA to regulate foreign-intelligence surveillance conducted by the Executive Branch within the United States. *See* Pl.'s Mot. at 15-16. Although that much is true, § 1806(f) is not "the mechanism that Congress has chosen for the protection of individual rights from overarching executive surveillance." *Id.* at 19. Rather, Congress achieved this objective "by

establishing a detailed process the Executive Branch must follow to obtain orders allowing it to collect foreign intelligence information without violating the rights of citizens of the United States." *Rosen*, 447 F. Supp. 2d at 543; *see, e.g.*, 50 U.S.C. §§ 1804-05; 1809; 1812; 1842; 1881a. Congress also created the FISC to administer FISA, *see* 50 U.S.C. § 1803, and put in place an extensive reporting structure. *See id.* §§ 1807-08, 1846, 1881f. This robust oversight framework is the "mechanism Congress has chosen" to serve the objectives that Plaintiff cites.

In short, nothing in the text or legislative history of § 1806(f) speaks clearly, unequivocally, directly, or in any way shape or form to displacing the state secrets privilege (or by the same token, the Government's statutory privileges), whether in the circumstances presented here, or otherwise.

3. Plaintiff's position is unsupported by other authority.

Plaintiff cites two district court decisions in support of its argument that § 1806(f) supersedes the state secrets privilege. Pl.'s Mot. at 19-20. But both cases were incorrectly decided, and neither supports the outcome Plaintiff seeks here.

In re NSA Telecomms. Records Litig., 564 F. Supp. 2d 1109 (N.D. Cal. 2008) held that § 1806(f) displaces the state secrets privilege, but the court did not consider whether the statute plainly and unequivocally expressed an intention to displace the privilege. Instead, it noted supposedly "striking" "similarities" between § 1806(f)'s procedures and those undertaken when the Government asserts the state secrets privilege. *Id.* at 1119. This analysis is inconsistent even with the test that Plaintiff advocates, *see* Pl.'s Mot. at 13-14, and overlooks that any similarities between the two procedures are superficial at best—if applied in this setting, they lead to diametrically opposed results, *see infra* at 31-32. Ultimately, *In re NSA Telecomms.* was vacated on other grounds. *Al-Haramain Islamic Foundation, Inc. v. Bush*, 705 F.3d 845 (9th Cir. 2012).

In *Jewel v. NSA*, 965 F. Supp. 2d 1090 (N.D. Cal. 2013), the court also erred and did not evaluate whether § 1806(f) plainly and unequivocally expresses an intent to displace the state secrets privilege. *See id.* at 1105-06. Moreover, subsequently—without reference to § 1806(f) or to *ex parte* proceedings thereunder—the court in *Jewel* upheld the Government's assertion of the state secrets privilege over classified sources and methods of Upstream surveillance. *See Jewel v. NSA*, 2015 WL 545925, at *5 (N.D. Cal. Feb. 10, 2015) (noting that "[t]he details of the Upstream collection process . . . are subject [to] the Government's assertion of the state secrets privilege"). Currently, the court in *Jewel* is reviewing privileged materials *ex parte*, not to determine the lawfulness of surveillance, or even to adjudicate the plaintiffs' standing, but to determine whether any of those materials can be disclosed to the plaintiffs in that case without placing national security at risk—more akin to the review required when evaluating an assertion of the state secrets privilege. *See Jewel v. NSA*, Tr. 48:10-19 (May 19, 2017) (Exh. D). Thus, neither the now-vacated opinion from *In re NSA Telecomms.*, nor the effectively-reconsidered opinion in *Jewel*, supports Plaintiff's position here.

Plaintiff also cites a number of statutes for the proposition that "Congress and the courts have a long-established and constitutional role to play in the handling of sensitive and classified information." Pl.'s Mot. at 17-19. But Plaintiff cites no authority for the proposition that these enactments, including various provisions concerning disclosure of intelligence information to Congress, *sub silentio* eliminate the constitutionally rooted prerogative of the Executive Branch to shield national security information that it determines is too sensitive to disclose. Hence, they provide no support for the idea that Congress would have done so when it enacted § 1806(f).

Indeed, FOIA, the Classified Information Procedures Act, ("CIPA"), 18 U.S.C. App. 3 §§ 1-16, and FISA, all cited by Plaintiff, demonstrate just the opposite. The Supreme Court has often warned against the risk of inadvertent yet harmful disclosures inherent in judicial review of

classified information, even "by [a] judge alone, in chambers." *Reynolds*, 345 U.S. at 10; *see also Clapper v. Amnesty Int'l, USA*, 568 U.S. 398, 412 n.4 (2013); *Tenet v. Doe*, 544 U.S. 1, 11 (2005). CIPA, FOIA, and FISA all accommodate the interest in protecting national security information against such risk in ways that § 1806(f), as Plaintiff construes it, would not.

FOIA exempts from disclosure any information that is properly classified, 5 U.S.C. § 552(b)(1), and judicial review of Executive classification decisions is highly deferential. *See, e.g.*, *Bowers v. U.S. Dep't of Justice*, 930 F.2d 350, 357 (4th Cir. 1991). Moreover, *in camera* review of the requested information "is not resorted to as a matter of course," *see*, *e.g.*, *Quinon v. FBI*, 86 F.3d 1222, 1228 (D.C. Cir. 1996), as Plaintiff urges under its reading of § 1806(f).

CIPA protects certain information from disclosure in criminal proceedings if the Government objects that it is classified. 18 U.S.C. App. 3 § 6(e)(1); *U.S. v. Rosen*, 487 F. Supp. 2d 703, 707 (E.D. Va. 2007) ("CIPA does not authorize a trial judge to second-guess the government's decision to classify information."). In certain circumstances the Government may then seek to delete the information or propose a substitute, "which may be accepted if fair to defendants, or if not accepted, the government may . . . refuse to allow the information's admission at trial [and] be subject to an appropriate sanction," *U.S. v. Rosen*, 520 F. Supp. 2d 786, 801-02 (E.D. Va. 2007), including dismissal of the indictment. 18 U.S.C. App. 3 § 6(e)(2). Thus, CIPA allows the Government to protect classified material in the same manner as does § 1806(f) when invoked in circumstances to which it properly applies, namely, in proceedings where the Government can forgo prosecution if ordered to disclose material, even to the court, that it judges too sensitive to release. The Government would be deprived of that ability were § 1806(f) applied in a situation such as this, where the Government, as the party defendant, does not have the option of dropping the case.

By the same token, Plaintiff is mistaken when it argues that its interpretation of § 1806(f) would require the Government to produce information "no more extensive" than the FISC itself requires in deciding whether to approve an application for surveillance. Pl.'s Mot. at 19. Plaintiff overlooks that FISA gives the Government the choice of forgoing an application if the Government determines that information required to support the application is too sensitive to risk disclosure. Plaintiff's reading of § 1806(f), which would deprive the Government of its ability to make such a determination, finds no support in FISA's legislative scheme.

4. Proceeding as Plaintiff advocates would endanger national security in exactly the manner condemned by the Supreme Court in *Amnesty International*.

Finally, although Plaintiff insists § 1806(f)'s procedures would yield the same result as the state secrets privilege "if the Attorney General attests to the harm that would flow from [disclosure]," Pl.'s Mot. at 18-19, the two procedures yield dramatically different outcomes. If the Court upholds the Government's claim of privilege, information subject to the privilege "is absolutely protected from disclosure—even for the purpose of *in camera* examination." *El-Masri*, 479 F.3d at 306. It is "remove[d] . . . from the proceedings entirely." *Id.* If, on the other hand, the Court proceeded as Plaintiff proposes, this would inevitably lead to the disclosure of whether Plaintiff was subject to surveillance or not, a fact subject to the Government's assertion of privilege here. *See* Classified NSA Decl. If the Court were to review *in camera* and *ex parte* evidence about "whether the NSA is intercepting, copying, and reviewing Wikimedia's international Internet communications," Pl.'s Mot. at 12-13, any decision rendered thereafter would reveal the substance of the classified material submitted to the Court: if the case were dismissed, that would reveal that Plaintiff had not been subject to surveillance; and if the case proceeded, that would reveal that Plaintiff had been.

This is the very danger against which the Supreme Court warned in *Amnesty International*, when it rejected a similar proposal that the Government disclose *in camera*

whether plaintiffs seeking to challenge surveillance under Section 702 had been subjects of such surveillance. 568 U.S. at 412 n.4. "[T]his type of hypothetical disclosure proceeding would allow a terrorist (or his attorney) to determine whether he is currently under U.S. surveillance simply by filing a lawsuit challenging the Government's surveillance program" as "the court's post disclosure decision about whether to dismiss the suit for lack of standing" necessarily would reveal whether he had been subject to surveillance. *Id.*

In sum, properly construed, § 1806(f) applies to situations in which the Government is using affirmatively information from electronic surveillance, and "ensures adequate protection of national security interests." H.R. Conf. Rep. No. 95-1720, at 32. In that setting, § 1806(f) procedures are invoked after surveillance has been acknowledged, and therefore no sensitive information is necessarily revealed by the court's decision following *ex parte* review. However, when invoked, as here, for the purpose, unintended by Congress, of establishing whether litigants were subject to surveillance in the first instance, it results in the very risks to national security that *Amnesty International* reminds courts they must avoid.

IV. ADDITIONAL GROUNDS REQUIRING THAT PLAINTIFF'S MOTION TO COMPEL BE DENIED

In addition to the conclusive effects of the DNI's and NSA's assertions of privilege, Plaintiff's motion should be denied because it (i) seeks information that is irrelevant to jurisdictional issues; (ii) seeks to impose undue burden and expense on the Government; and (iii) represents improper attempts to use requests for admissions as discovery devices.

A. Lack of Relevance

In numerous instances Plaintiff's discovery requests call for information having no bearing on the question of jurisdiction. For example, in response to Interrogatory Nos. 6 and 8 Plaintiff demands a classified explanation of the term "Internet transaction," as defined by the NSA. Yet Plaintiff does not explain why that information has any bearing on the "key facts"

underlying its standing argument—the alleged ubiquity of its communications, technical rules of how the Internet works, and the fact that Upstream collection takes place somewhere on the Internet backbone. *See Wikimedia*, 857 F.3d at 210-11. Plaintiff asserts that "[t]hese requests bear on [its] showing of how Upstream surveillance results in the copying and review of [its] communications," Pl.'s Mot. at 28, but it offers no explanation as to why that would be so.

Similarly, Plaintiff's requests regarding the volume of communications subject to Upstream surveillance, Interrogatory Nos. 14-15; RFP No. 10, and the NSA's Section 702 Targeting Procedures, RFP No. 18, RFA Nos. 28-30, are unmoored from its own theory of standing. The volume of communications subject to Upstream surveillance is unrelated to the alleged volume and distribution of Wikimedia's communications, the technical rules of the Internet, or the location(s) of Upstream surveillance. NSA Targeting Procedures address the sources of information and analytic techniques used to ensure that persons targeted for surveillance under Section 702 are non-U.S. persons reasonably believed to be located abroad; they are not concerned with the means or methods of Upstream collection.

Plaintiff argues that its requests for authentication of purportedly classified documents, RFA Nos. 16-21, 25-30, are relevant because "[e]ven a passing review of these documents show that they relate to the NSA's surveillance of Wikimedia's communications." Pl.'s Mot. at 30. That argument stumbles over the fact that the documents, on their face, either make no reference to Upstream surveillance, fail to mention the NSA, and/or say nothing about Wikimedia.

B. Undue Burden

Any suggestion by Plaintiff that the Government should be required to produce unclassified (*i.e.*, redacted) versions of the documents responsive to RFP Nos. 21 and 22 should be rejected on grounds of undue burden. *See* Fed. R. Civ. P. 26(b)(1), (b)(2)(C)(iii). Because the responsive documents are classified FISC opinions and orders and submissions, these requests

implicate the interests of multiple intelligence agencies such as the NSA, CIA, FBI, and the National Counter-Terrorism Center. Processing them for public disclosure would require an "extremely time consuming and resource intensive" "line-by-line" review of each document through an iterative, intra- and inter-agency process to ensure protection of still-classified information. Bernick Decl. ¶¶ 8-12. To complete this process on a scale of over 10,000 pages of documents is likely to take "much longer" than one year and could take "several years." *Id.* ¶¶ 7, 14, 16. The burden would not be significantly diminished even if the review were limited to documents not previously subjected to classification review, because the "vast majority" of the documents have not undergone such review. *Id.* ¶ 15. Only if Plaintiff withdrew RFP No. 22 and narrowed RFP No. 21 to seek those FISC orders that had been previously subject to such a review "would the drain" on Government "resources be significantly eased." *Id.*

The burden of preparing unclassified versions of the documents responsive to RFP Nos. 21 and 22 far outweighs any likely benefit in terms of producing relevant evidence. Fed. R. Civ. P. 26(b)(1). That is so principally because Plaintiff insists on production of all 10,000 pages of documents, without regard to whether they contain information about the sources and methods and operational details of Upstream collection that Plaintiff desires. *See Transamerica Life Ins. Co. v. Moore*, 274 F.R.D. 602, 609 (E.D. Ky. 2011) (omnibus requests for general categories of documents are considered overbroad and unduly burdensome); *see also* Pl.'s Mot. at 29.[16] What is more, because these details are the very kind of classified information that would be redacted from unclassified versions of the documents, the chances that this enormous investment of personnel time and resources will result in the discovery of relevant evidence are close to nil.

[16] Plaintiff's assertion that "these documents broadly and variously describe how and where Upstream surveillance is conducted," Pl.'s Mot. at 29, is necessarily made without basis in knowledge, because Plaintiff has never had access to these classified materials.

Even if the categories of documents that Plaintiff seeks could be considered relevant on their face, many of the requests are overbroad and unduly burdensome insofar as they call for documents dated as long ago as 2008. *See* NSA Resps. to RFA Nos. 10, 13, 14, 16, 21-24. To establish standing to sue for prospective equitable relief, the sole relief it prays for, *see* 1st Am. Compl. at 55-56, Plaintiff must demonstrate that its communications are subject to Upstream collection activities *today*. *See Nanni v. Aberdeen Marketplace, Inc.*, 878 F.3d 447, 454 (4th Cir. 2017). Evidence of how Upstream surveillance may have been conducted a decade ago would be of little to no value when it comes to resolving that issue.

C. Improper Use of Requests for Admissions as Discovery Devices

Plaintiff propounded RFA Nos. 6-10, 13-15, 34-38, and 40 to elicit evidence regarding matters, such as the location(s) of Upstream surveillance, about which Plaintiff has no other sources of competent proof. RFAs are not meant for such use as general discovery devices. *See, e.g., Graphic Sec. Sys. Corp. v. Nautilus Sec.*, 2010 WL 11534374, at *2 (D.S.C. Aug. 20, 2010); *Erie Ins. Prop. & Cas. Co. v. Johnson*, 272 F.R.D. 177, 183 (S.D.W. Va. 2010); *Frontier-Kemper Constructors, Inc. v. Elk Run Coal Co.*, 246 F.R.D. 522, 531 (S.D.W. Va. 2007). For this reason, too, Plaintiff's motion to compel responses to these requests should be denied.[17]

CONCLUSION

For the reasons stated above, the Government's assertions of the state secrets privilege, and its statutory privileges, should be sustained, and Plaintiff's motion to compel denied.

[17] Plaintiff argues that the Government's responses to its RFAs were "improper." Pl.'s Mot. at 32-33. But having objected to Plaintiff's RFAs on grounds of privilege, and/or their unauthorized use as discovery devices, the Government discharged its obligations and was not required to give any further response at all, *see* Fed. R. Civ. P. 36(a)(3), (5); *Lynn v. Monarch Recovery Mgmt., Inc.*, 285 F.R.D. 350, 363 (D. Md. 2012), even though it endeavored to respond to the greatest extent possible without revealing classified information. *See, e.g.*, NSA Resps. to Pl.'s RFA Nos. 6, 8, 10. Plaintiff's argument boils down to a complaint that the Government did not go far enough in *exceeding* its obligations under Rule 36, and should be rejected.

Dated: April 27, 2018

Respectfully submitted

CHAD A. READLER
Acting Assistant Attorney General

ANTHONY J. COPPOLINO
Deputy Branch Director

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

RODNEY PATTION
Senior Trial Counsel

JULIA A. BERMAN
TIMOTHY A. JOHNSON
OLIVIA HUSSEY-SCOTT
Trial Attorneys

U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave., N.W., Room 6102
Washington, D.C. 20001
Phone: (202) 514-3358
Fax: (202) 616-8470
Email: james.gilligan@usdoj.gov

Counsel for Defendants