IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

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

MEMORANDUM OPINION

At issue in this First and Fourth Amendment suit is plaintiff's motion to compel defendants to respond to discovery requests regarding defendant National Security Agency's ("NSA") Upstream surveillance program. Specifically, plaintiff served 84 discovery requests on defendants in an effort to establish that at least one of plaintiff's communications has been intercepted, copied, and reviewed by defendants. Defendants have objected to 53 of these requests on the basis of the common law state secrets privilege and other statutory privileges, arguing that the information plaintiff seeks, if disclosed, reasonably could be expected to result in exceptionally grave damage to U.S. national security. Plaintiff now moves for an order compelling defendants to produce any information responsive to plaintiff's requests, contending that the Foreign Intelligence Surveillance Act ("FISA")[1] displaces the common law state secrets privilege and establishes procedures for the *ex parte* and *in camera* review of sensitive national security information. These issues have been fully briefed and argued and are now ripe for disposition.

[1] 50 U.S.C. § 1801, *et seq.*

I.

A brief summary of the statutory framework pertinent to defendants' electronic surveillance efforts provides context necessary for resolution of the question presented in this case. In 1978, Congress enacted FISA in response to growing concerns about the Executive Branch's use of electronic surveillance. Specifically, Congress sought through FISA to accommodate U.S. national security interests in obtaining intelligence about foreign powers while also providing meaningful checks on the Executive Branch's ability to conduct that surveillance. In this respect, FISA created a "secure framework by which the Executive Branch may conduct legitimate electronic surveillance for foreign intelligence purposes within the context of this Nation's commitment to privacy and individual rights." S. Rep. No. 604, pt. 1, 95th Cong. 1st Sess. 15 (1977), reprinted in U.S.Code Cong. & Admin.News 1978, pp. 3904, 3916.

A central component of this framework is the U.S. Foreign Intelligence Surveillance Court ("FISC"). FISC, a tribunal composed of eleven federal district judges designated by the Chief Justice of the U.S. Supreme Court, is charged with the review of applications for electronic surveillance. *See* 50 U.S.C. § 1803(a). FISA provides that, with limited exceptions, the Executive Branch cannot conduct surveillance of a foreign power or its agents absent prior FISC authorization. To obtain FISC authorization for electronic surveillance, the Attorney General must personally approve an application for surveillance, which must (i) comport with FISA's procedural requirements and (ii) establish probable cause to believe that the target of electronic surveillance is a foreign power or an agent of a foreign power and that each of the facilities at which electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power. *Id.* § 1805

FISA also establishes rules governing the use of information obtained through electronic surveillance. *See id.* § 1806. Specifically, if the Government, including any State or political subdivision, intends to "enter into evidence or otherwise use or disclose" at any proceeding information obtained through electronic surveillance against an "aggrieved person"—that is, any person who has been the subject of electronic surveillance—the Government must first "notify the aggrieved person and the court or other authority" of its intent to so disclose or use the information. *Id.* §§ 1806(c),(d). The person against whom the evidence is to be introduced may then move to suppress the evidence obtained through electronic surveillance on the grounds that (i) "the information was unlawfully acquired" or (ii) "the surveillance was not made in conformity with an order of authorization or approval." *Id.* § 1806(e). FISA establishes specific procedures that courts must follow in the event (i) that the government notices its intent to use electronic surveillance information, (ii) that an aggrieved person files a motion to suppress or (iii) that an aggrieved person files "any motion . . . pursuant to any other statute or rule of the United States . . . to discover, obtain, or suppress" information obtained from electronic surveillance. *Id.* § 1806(f). Specifically, the court

> shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure . . . 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 . . . ."

Id.

On the basis of its *ex parte* and *in camera* review of the materials at issue, the court must determine "whether the surveillance of the aggrieved person was lawfully authorized and conducted." *Id.* FISA permits courts making this determination to disclose to the aggrieved person portions of the application, order, or other materials "only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." *Id.* If, in the end, the court

determines that the surveillance was not lawfully authorized or conducted, the court must suppress the unlawfully obtained evidence or otherwise grant the motion of the aggrieved person. *Id.* § 1806(g). If, on the other hand, the surveillance was lawfully authorized and conducted, the court "shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure." *Id.*

In addition to mandating specific procedures governing the use of information obtained through electronic surveillance, FISA establishes additional checks on the Executive's use of electronic surveillance. Two such checks come by way of criminal sanctions and a civil cause of action. Specifically, FISA imposes criminal penalties on any person who intentionally "engages in electronic surveillance under color of law except as authorized by [FISA]" or "discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by [FISA.]" *Id.* § 1809(a)(1)-(2). FISA also provides a civil cause of action to any "aggrieved person . . . who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 1809 . . . against any person who committed such violation . . . ." *Id.* § 1810.

In 2008, thirty years after FISA's enactment, Congress passed the FISA Amendments Act ("FAA"), which establishes additional procedures and requirements for the authorization of surveillance targeting persons located outside the United States. *See* 50 U.S.C. § 1881a-g. Specifically, § 702 of the FAA[2] provides that the Attorney General and the Director of National Intelligence may jointly authorize, for up to one year, the "targeting of [non-U.S.] persons reasonably believed to be located outside the United States to acquire foreign intelligence

[2] 50 U.S.C. § 1881a.

information" if the FISC approves "a written certification" submitted by the government attesting, *inter alia*, (i) that a significant purpose of the acquisition is to obtain foreign intelligence information and (ii) that the acquisition will be conducted "in a manner consistent with the [F]ourth [A]mendment" and the targeting and minimization procedures required by statute. 50 U.S.C. § 1881a(b),(g). To approve such a certification, the FISC must determine that the government's targeting procedures are reasonably designed:

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

Unlike FISA, these FAA procedures do not require the FISC to determine that probable cause exists to believe that the target of electronic surveillance is a foreign power and that each of the facilities at which electronic surveillance is directed is being used or is about to be used by a foreign power.

The recent release of public reports and declassification of FISC opinions have revealed additional details regarding the collection of communications under § 702. For example, the government has disclosed that it conducts § 702 surveillance through two programs—PRISM and Upstream surveillance. *See* Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* 7 (2014) ("PCLOB Report"). The program at issue here, Upstream surveillance, involves

collection of communications of persons reasonably believed to be outside of the United States "with the compelled assistance . . . of the providers that control the telecommunications backbone over which [telephone and Internet] communications transit." *Id.* at 35. In this respect, "[t]he government 'tasks' certain 'selectors,' such as telephone numbers or email addresses, that are associated with targeted persons, and it sends these selectors to electronic communications service providers to begin acquisition." *Id.* at 7. The providers then assist the government in the collection of the communications associated with those selectors. *See id.*

II.

With this statutory framework in mind, it is appropriate to turn to the facts and procedural history in this case. Plaintiff Wikimedia Foundation, a non-profit organization based in San Francisco, California, operates several "wiki"-based projects and provides the contents of those projects to individuals around the world free of charge. Defendant National Security Agency/Central Security Service ("NSA") is the U.S. government agency responsible for conducting the surveillance at issue in this case. Defendant Office of the Director of National Intelligence ("ODNI") is the agency responsible for directing the activities of the U.S. intelligence community, including the NSA, and defendant Department of Justice ("DOJ") is one of the government agencies responsible for overseeing electronic surveillance. Several individual defendants are also named in their official capacities, including the Director of the NSA and the Chief of the Central Security Service, the Director of National Intelligence, and the Attorney General of the United States.

On June 22, 2015, plaintiff, along with eight other organizations,[3] filed the Amended Complaint in this suit, challenging the legality of defendants' Upstream surveillance program pursuant to § 702 of the FAA. The Amended Complaint alleges that this program violates (i) the Administrative Procedure Act ("APA"), (ii) the Fourth Amendment to the Constitution, (iii) the First Amendment to the Constitution, and (iv) Article III of the Constitution. The Amended Complaint seeks (i) a declaration that Upstream surveillance violates the APA and the Constitution and (ii) an injunction permanently enjoining defendants from continuing Upstream surveillance.

On August 6, 2015, defendants filed a Motion to Dismiss pursuant to Rule 12(b)(1), Fed. R. Civ. P., arguing that none of the plaintiff organizations plausibly alleged that they were injured by the interception, copying and review of online communications via the Upstream surveillance program and thus plaintiffs lacked Article III standing to contest the legality of the program. Subsequently, on October 23, 2015, an Order and a Memorandum Opinion issued, concluding that the allegations in the Amended Complaint were too speculative to establish Article III standing and granting defendants' motion to dismiss as to all plaintiffs. *See Wikimedia Found., et al., v. Nat'l Sec. Agency*, 143 F. Supp. 3d 344, 356-57 (D. Md. 2015), *aff'd in part, vacated in part, and remanded by* 857 F.3d 193 (4th Cir. 2017). Thereafter, plaintiffs appealed and the Fourth Circuit issued an opinion affirming in part, vacating in part, and remanding the case to the district court for further consideration. *See Wikimedia Found., et al., v. Nat'l Sec. Agency*, 857 F.3d 193 (4th Cir. 2017). Specifically, the Fourth Circuit concluded that although the eight other organizations had failed to allege injuries sufficient to satisfy the requirements of Article III standing, Wikimedia Foundation had alleged facts "sufficient to make plausible the conclusion that the NSA is

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

intercepting, copying, and reviewing at least some of Wikimedia's communications." *Wikimedia Found, et al..*, 857 F.3d at 210.

Shortly after the Fourth Circuit remanded the case to the district court for further proceedings, the parties submitted briefs on how to proceed in the case. Defendants indicated their intent to continue to challenge plaintiff's Article III standing and argued that any discovery should be bifurcated to allow for resolution of the standing question prior to resolution of the merits. Plaintiff opposed defendants' proposed discovery plan, contending that the jurisdictional facts at issue here are so intertwined with the merits as to require simultaneous discovery and summary judgment briefing on both questions. On October 3, 2017, an Order issued, directing the parties to conduct a limited five-month period of jurisdictional discovery prior to full discovery on the merits. *See Wikimedia Found. v. Nat'l Sec. Agency*, 1:15-cv-662 (D. Md. Oct. 3, 2017) (Order).

The parties then proceeded to engage in the limited discovery as directed. Plaintiff served 84 requests for admission, interrogatories, and requests for production on defendants, seeking what plaintiff describes as three broad categories of information: (i) direct evidence that Wikimedia has been surveilled, (ii) definition of key terms used in describing Upstream surveillance to the public, and (iii) evidence concerning the scope and breadth of Upstream surveillance.[4] Defendants responded to several of these discovery requests by producing 500 pages of unclassified documents, but objected to 53 of plaintiff's requests on the basis of privilege. In particular, defendants asserted that the information sought by plaintiff was protected by the common law state secrets privilege and other statutory privileges regarding the protection of national security information. In this respect, defendants submitted the unclassified declaration of Daniel Coats, the Director of National Intelligence, formally invoking the state secrets privilege on the basis of

[4] That these interrogatories covered both standing and merits matters is neither inappropriate nor unexpected, as these matters may well be inextricably entwined.

his personal consideration of the risks associated with disclosure of the information plaintiff seeks. Defendants also submitted a classified declaration of George C. Barnes, the Deputy Director of the NSA, providing additional detail concerning the harm to national security that would be caused by disclosure of the information contained in plaintiff's discovery requests.

Subsequently, on March 26, 2018, plaintiff filed the Motion to Compel at issue here pursuant to Rule 37(a)(3), Fed. R. Civ. P. Plaintiff contends that where, as here, a party moves to discover material relating to electronic surveillance, the court must follow FISA's § 1806(f) procedures and conduct an *ex parte* and *in camera* review of the materials relating to electronic surveillance. Plaintiff argues that these procedures apply despite defendants' assertion of state secrets privilege because in enacting FISA, Congress intended to displace the common law state secrets privilege. And even assuming the state secrets privilege was not displaced by FISA, plaintiff argues that the privilege does not bar disclosure of the information at issue here given the amount of information concerning Upstream surveillance already in the public record.

Defendants oppose plaintiff's motion, arguing (i) that § 1806(f) does not apply where, as here, plaintiff has not yet established that it is the target of electronic surveillance and (ii) that even assuming § 1806(f) does apply here, there is no clear statement indicating Congress's intent to displace the common law state secrets privilege through enactment of FISA. Finally, defendants contend that the government's assessment of the national security risks associated with disclosure of the information concerning plaintiff's discovery requests is entitled to deference and that plaintiff's arguments to the contrary are baseless.

III.

A threshold question that must be addressed is whether the *ex parte* and *in camera* review procedures established in § 1806(f) apply where, as here, a plaintiff is seeking classified discovery

to establish that the plaintiff's communications were unlawfully seized and searched. Analysis of this question properly begins with the terms of that statute. Section 1806(f) provides, in pertinent part:

> Whenever a court or other authority is notified pursuant to subsection (c) or (d) of this section, or whenever a motion is made pursuant to subsection (e) of this section, or 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 orders or other materials relating to electronic surveillance . . . the United States district 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. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

50 U.S.C. § 1806(f). The statute further defines "aggrieved person" as "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance." *Id.* § 1801(k).

This statutory text points persuasively to the conclusion that § 1806(f) procedures do not apply where, as here, a plaintiff has not yet established that it has been the subject of electronic surveillance. Specifically, the text of § 1806(f) identifies only three circumstances in which its procedures apply: (i) when the government notifies the court that it plans to introduce evidence obtained through electronic surveillance, (ii) when an aggrieved person moves to suppress information obtained through electronic surveillance, and (iii) when an aggrieved person makes "any motion or request . . . pursuant to any other statute or rule of the United States . . . to discover or obtain . . . materials relating to electronic surveillance." *Id.* Here, (i) and (ii) are clearly not met. The government has not noticed its intent to use or disclose information obtained through electronic surveillance, and plaintiff has not filed a motion to suppress any such information.

Accordingly, the only possible § 1806(f) situation applicable here is (iii), the third circumstance that may trigger § 1806(f). But importantly, § 1806(f) provides that this third situation applies only when the motion or request at issue "is made by an *aggrieved person*[,]"[5] namely "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance."[6] In this regard, the text of § 1806(f) makes clear that a party's status as an "aggrieved person," or the subject of surveillance, is a precondition to the application of § 1806(f)'s procedures; unless and until a party has adduced evidence that it has been the subject of electronic surveillance, a party's motion cannot trigger § 1806(f)'s *ex parte* and *in camera* review procedures.

This interpretation of the text is confirmed by the nature of § 1806(f)'s procedures once invoked. Specifically, § 1806(f)'s procedures require courts to engage in *ex parte* and *in camera* review of orders or other materials relating to surveillance to determine whether the surveillance at issue "was lawfully authorized and conducted." *Id.* § 1806(f). A determination that surveillance was lawfully authorized and conducted cannot occur unless a determination has previously been made that the surveillance at issue did, in fact, occur. Put differently, it is impossible to determine the lawfulness of surveillance if no surveillance has actually occurred. Thus, the text of § 1806(f) points persuasively to the conclusion that Congress intended § 1806(f) procedures to apply only after it became clear from the factual record that the movant was the subject of electronic surveillance.

Had Congress instead intended § 1806(f) to be a vehicle for parties to determine whether they were the target of electronic surveillance, one would expect to see language requiring courts

---

[5] *Id.*

[6] *Id.* § 1801(k).

to review materials relating to electronic surveillance to determine whether "electronic surveillance occurred," or requiring the government to affirm or deny the existence of any surveillance. Indeed, Congress has used precisely this language elsewhere in the U.S. Code. Specifically 18 U.S.C. § 3504, which was enacted eight years prior to FISA in 1970, provides that where a party claims evidence is admissible because the evidence is the product of an unlawful act, such as warrantless wiretapping, "the opponent of the claim shall affirm or deny the occurrence of the alleged unlawful act[.]" 18 U.S.C. § 3504. This provision demonstrates that Congress knew how to draft language requiring the government to affirm or deny the existence of some fact when Congress sought to do so. But importantly, § 1806(f) does not adopt this or similar language requiring an affirmation or denial of the fact of surveillance upon motion by an aggrieved person; rather, § 1806(f) provides that, upon a motion made by an aggrieved party, the court will determine whether the surveillance "was lawfully authorized and conducted." To assign meaning to this textual variation demands that § 1806(f) be interpreted to require *ex parte* and *in camera* review of the lawfulness of surveillance only after the individual has adduced evidence that he has been the target of electronic surveillance. *Cf. Lorillard v. Pons*, 434 U.S. 575, 584 (1978) (finding that Congress did not intend to apply the standards from one statute to a later-enacted statute where significant differences existed in the text of the two statutes).

Consideration of the other circumstances in which § 1806(f) procedures apply further bolsters the conclusion reached here. It is axiomatic that where, as here, "general words follow specific words in a statutory enumeration, the general words are usually construed to embrace only objects similar in nature to those objects enumerated by the preceding specific words." *Yates v. United States*, 135 S.Ct. 1074 (2015) (quoting *Washington State Dept. of Social & Health Servs. v. Guardianship Estate of Keffeler*, 537 U.S. 371, 384 (2003) (internal quotation marks omitted)).

In *Begay v. United States*, 553 U.S. 137, 142-43 (2008), the Supreme Court relied on this principle to determine whether specific crimes were covered by the statutory phrase "any crime . . . that . . . is burglary, arson, or extortion, involves use of explosives, or otherwise involves conduct that presents a serious potential risk of physical injury to another[.]" The Supreme Court reasoned that the enumeration of specific crimes—that is, burglary, arson, extortion, and use of explosives—indicated that the broadly worded "otherwise involves" provision covered "only similar crimes, rather than every crime that 'presents a serious potential risk of physical injury to another.'" *Id.* at 142.

The statutory provision at issue here—§ 1806(f)—is structured in precisely the same way as the provision at issue in *Begay*. Specifically, like the provision at issue in *Bergay*, § 1806(f) enumerates two specific situations covered by its procedures—namely, when the government provides notice pursuant to § 1806(c)-(d) and when a person against whom evidence is to be introduced moves to suppress that evidence pursuant to § 1806(e)—followed by a broadly-worded more general provision that also triggers § 1806(f)—namely, "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 orders or other materials relating to electronic surveillance . . . ." *Id.* As in *Bergay*, this broadly-worded, more general provision must be interpreted in light of the specifically enumerated provisions listed before it. And importantly, in each of these two specific situations, there is clear evidence that electronic surveillance has occurred; the only question is whether the evidence derived from the electronic surveillance may properly be disclosed.[7] Thus,

[7] This common thread uniting the situations in which § 1806(f) applies is further highlighted by the legislative history of this provision. Specifically, the Senate Report notes additional examples of instances in which § 1806(f)'s procedures apply, including "whenever an individual makes a motion pursuant to . . . 18 U.S.C. § 3504 . . . to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance . . . ." S. Rep. 95-701, 63, 1978 U.S.C.C.A.N. 3973, 4032. In this respect, the Senate Report explained that a defendant could "quer[y] the

to "avoid ascribing to one word a meaning so broad that it is inconsistent with its accompanying words" and to avoid "giving unintended breadth to the Acts of Congress[,]" it is necessary to interpret the final provision of § 1806(f) as similarly requiring evidence of the fact of electronic surveillance. *Gustafson v. Alloyd Co.*, 513 U. S. 561, 575 (1995).

Support for the conclusion reached here is found not solely in the text of § 1806(f) itself, but also in the caption of § 1806 and the general structure of the provision. Although "headings are not commanding," the Supreme Court has recognized that headings can "supply cues" that Congress did not intend a particular meaning of the statute. *Yates v. United States*, 135 S. Ct. 1074, 1083 (2015). Section 1806's heading—use of information—suggests that Congress did not intend §1806(f) to apply in situations where, as here, it is yet unclear whether electronic surveillance even occurred. Rather, the heading suggests that Congress intended the provisions of § 1806 to apply where evidence already establishes the fact of surveillance, and the central dispute is instead how, and whether, information obtained via that electronic surveillance can be used or disclosed in a proceeding.

Finally, as the Supreme Court has recognized, "[i]t is axiomatic that statutes in derogation of the common law should be narrowly construed[.]" *Badaracco v. C.I.R.*, 464 U.S. 386, 403 n.3 (1984). In this case, as plaintiff notes, § 1806(f) seems on its face to conflict with traditional principles of common law, namely the common law state secrets privilege. Specifically, the mandatory *ex parte* and *in camera* review procedures established in § 1806(f), in situations in which these procedures apply, likely displace the common law process whereby courts review the government's assertion of the state secrets privilege to avoid disclosure of information potentially harmful to national security. Given this, traditional principles of statutory interpretation counsel

---

government under 18 U.S.C. § 3504," "discover[] that he has been intercepted by electronic surveillance" and then move to suppress or to discover or obtain information related to that surveillance.

that FISA must be narrowly construed so as to avoid excessive displacement inconsistent with Congress's intent. To interpret the text of § 1806(f) broadly, as plaintiff here suggests, to encompass not just motions raised by parties who have adduced evidence that they are "aggrieved persons," but also motions by parties who simply allege that they are "aggrieved persons," would do precisely this, namely displace the common law to an extent neither contemplated nor intended by Congress.

In an attempt to avoid this conclusion, plaintiff contends that the allegations contained in the complaint are sufficient to establish that plaintiff is an "aggrieved person" within the meaning of § 1806(f). Specifically, defendant cites to the Fourth Circuit's determination that plaintiff's complaint alleges sufficient facts "to make plausible the conclusion that the NSA is intercepting, copying, and reviewing at least some of [plaintiff's] communications" and contends that this plausibility determination is sufficient standing alone to require invocation of § 1806(f)'s procedures. *Wikimedia Found., et al.*, 857 F.3d at 211. But the Fourth Circuit concluded that plaintiff had sufficiently alleged injury-in-fact for the purposes of surviving a motion to dismiss; the Fourth Circuit never considered the requisite showing of "aggrieved person" status to trigger the earlier procedures outlined in § 1806(f). *Id.* at 207-11. As such, the Fourth Circuit's determination in *Wikimedia* does not answer the question raised here—namely what showing is required prior to invocation of § 1806(f) procedures.

Notably, the only circuit authority to consider this latter question—what a party must show to establish his or her "aggrieved person" status and invoke § 1806(f)—recognized that a party may not trigger § 1806(f) procedures unless and until the party has adduced evidence of its "aggrieved person" status. Specifically, in *ACLU Foundation of Southern California v. Barr*, 952 F.2d 457 (D.C. Cir. 1991), the D.C. Circuit reversed the district court's dismissal of the plaintiffs'

First Amendment claim based on the government's surveillance of plaintiffs' communications. In denying the motion to dismiss, the D.C. Circuit reasoned that "legitimate concerns about compromising ongoing foreign intelligence investigations" are more properly considered at the summary judgment stage, not upon the pleadings. *Id.* at 469. In this respect, the D.C. Circuit explained that plaintiffs challenging alleged unlawful electronic surveillance must survive summary judgment—that is, they must adduce evidence sufficient to prove the existence of a genuine dispute about the fact of ongoing surveillance before the court applies § 1806(f) procedures. *Id.* The D.C. Circuit recognized that "in the usual case some discovery is permitted before the court rules on a motion for summary judgment," but importantly, the D.C. Circuit noted that "normal rules regarding discovery must be harmonized with FISA and its procedures, notably 1806(f)." *Id.* In this regard, The D.C. Circuit further explained that:

> even plaintiffs who defeat summary judgment motions would not be entitled to obtain any of the materials relating to the authorization of the surveillance or the evidence derived from it unless the district court, in an *ex parte, in camera* proceeding, first determined that the surveillance was not "lawfully authorized and conducted."

Id. This analysis in *Barr* makes clear that the D.C. Circuit contemplated the conclusion reached here, namely that in order to trigger § 1806(f) procedures, a plaintiff must first adduce evidence sufficient at least to create a genuine dispute as to whether the plaintiff has been the target of electronic surveillance in the past or whether electronic surveillance is ongoing.

Plaintiff next argues that to require a plaintiff to adduce evidence of surveillance to demonstrate his or her "aggrieved person" status would necessarily mean that a plaintiff could not do so unless the government affirmatively acknowledges the fact of surveillance. And to require the government affirmatively to acknowledge the fact of surveillance prior to invocation of § 1806(f) procedures, plaintiffs contend, would be inconsistent with other provisions in the statute, namely the civil cause of action established in § 1810.

This argument fails to persuade because it mischaracterizes both (i) the requirements for establishing "aggrieved person" status and (ii) the nature of the civil remedy established in § 1810. To begin with, affirmative government acknowledgement of surveillance of a specific target is not the only means by which a plaintiff can establish evidence of his or her "aggrieved person" status. Indeed, courts have recognized that plaintiffs can "rely on many non-classified materials, including present and future public disclosures of the government or [telecommunications providers] on the alleged NSA programs" to establish that they have been the target of electronic surveillance. *Hepting v. AT&T Corp., et al.*, 439 F. Supp. 2d 974, 998 (N.D. Cal. 2006). Thus, to require a plaintiff to adduce evidence of surveillance to demonstrate his or her "aggrieved person" status does not necessarily require that the government affirmatively acknowledge the fact of surveillance.

And even assuming, *arguendo*, that affirmative government acknowledgment was the only means by which a plaintiff could prove his or her "aggrieved person" status, this requirement would not be inconsistent with the remedy established in § 1810. That section provides a civil remedy to "[a]n aggrieved person . . . who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 1809." 50 U.S.C. § 1810. Plaintiff argues that to require government acknowledgement of surveillance prior to invocation of § 1806(f) procedures would render § 1810 a nullity because plaintiff's access to the remedy against the government would be dependent entirely on cooperation by the government. This argument is unpersuasive; courts have made clear that § 1810 is not actually a remedy against the government because § 1810 does not contain an explicit waiver of sovereign immunity. *See Al-Haramain Islamic Found., Inc. v. Obama*, 705 F.3d

845, 854 (9th Cir. 2012).[8] Instead, § 1810 provides a remedy against intelligence agents who engage in unlawful electronic surveillance or who disclose information obtained from unlawful surveillance in their personal, not official, capacities. In this respect, the civil cause of action in § 1810 is premised upon the individual agent's "violation of section 1809[,]" which establishes criminal penalties for unlawful surveillance. *Al-Haramain*, 705 F.3d at 854 (quoting 50 U.S.C. 1810).[9] There is no reason to believe that the government would be unwilling to cooperate in acknowledging that an individual agent conducted unlawful surveillance in his individual capacity. Indeed, to the extent that § 1810 is intended to track an individual agent's criminal liability, the government will necessarily acknowledge, and indeed prove, the fact of surveillance through a criminal prosecution of that individual agent.

Finally, plaintiff cites to one case in which a district court found that the plaintiffs "alleged enough to plead 'aggrieved person' status so as to proceed to the next step in proceedings under FISA sections 1806(f) and 1810." *In re NSA Telecommc'ns Records Litig.*, 595 F.Supp.2d 1077, 1085-86 (N.D. Cal. 2009). But in reaching this conclusion—namely that the allegations in plaintiff's complaint were sufficient to invoke § 1806(f) procedures—the court did not conduct an in-depth analysis of the text or indeed even of the legislative history of FISA. Instead, the *In re NSA Telecommunications Records Litigation* court imported a standard from the Ninth Circuit's analysis of claims pursuant 18 U.S.C. § 3504.[10] Section 3504 provides, in relevant part, that "upon a claim by a party aggrieved that evidence is inadmissible because it is the primary product of an

---

[8] *See also Whitaker v. Barksdale Air Force Base*, 2015 WL 574697, *7 (W.D. La. Feb. 11, 2015) (agreeing with the "extensive analysis" in *Al-Haramain*).

[9] *See also* H.R. Conf. Rep. No. 95-1720 (noting that the cause of action in § 1810 is afforded "to any aggrieved person about whom information has been disclosed or used in violation of the criminal penalty provisions" and that "civil liability of intelligence agents under this act should coincide with the criminal liability.").

[10] 18 U.S.C. 3504

unlawful act . . . , the opponent of the claim shall affirm or deny the occurrence of the alleged unlawful act." 18 U.S.C. § 3504. In *United States v. Alter*, 482 F.2d 1016 (9th Cir. 1974), the Ninth Circuit concluded that § 3504's requirement to affirm or deny the occurrence of the alleged unlawful act is triggered where the party aggrieved makes a "prima facie showing that good cause exists to believe" the individual was subject to illegal surveillance. *Id.* at 1026.

Plaintiff's reliance on *In re NSA Telecommunications Records Litigation* and its application of the § 3504 standard in the FISA context is unpersuasive because § 3504 is different from § 1806(f) in significant ways. Notably, although both § 1806(f) and § 3504 use the term "aggrieved," § 1806(f), unlike § 3504, incorporates a statutory definition of an "aggrieved person," which specifies that an "aggrieved person" is "a person who is the target of an electronic surveillance" or "whose communications or activities were subject to surveillance[.]" 50 U.S.C. § 1801(k). As such, while a party can claim to be aggrieved for the purposes of § 3504 through a "mere assertion"[11] that unlawful surveillance has occurred, § 1806(f) requires that the person has actually been a target of electronic surveillance or has been subject to surveillance before that individual can trigger the *ex parte* and *in camera* review procedures outlined in § 1806(f).

Moreover, the reasoning in support of the low burden in the § 3504 context does not apply here. Specifically, in analyzing § 3504, courts have reasoned that the government's obligation to affirm or deny the occurrence of unlawful surveillance is triggered by the mere assertion of unlawful wiretapping because "requiring the government to affirm or deny the existence of illegal surveillance of witnesses imposes only a minimal additional burden upon the government." *Vielguth*, 502 F.2d at 1259 n.4 (citing *In re Evans*, 452 F.2d at 1247). But this reasoning is inapplicable here because § 1806(f) requires much more than a simple affirmation or denial by the

[11] *United States v. Vielghth*, 502 F.2d 1257, 1258 (9th Cir. 1974) (quoting *In re Evans*, 452 F.2d 1239, 1247 (1971)).

government. Section 1806(f) procedures, once triggered, require the court to review *ex parte* and *in camera* all of the relevant materials relating to electronic surveillance—in this case, potentially 10,000 pages of documents—to determine the lawfulness of the surveillance. The reasoning justifying the low burden in § 3504 is thus inapplicable here where a much higher burden is associated with the applicable procedures. Given that the *In re NSA Telecommunications Records Litigation* court, in interpreting the requirements of § 1806(f), relied on a standard imported from 18 U.S.C. § 3504, which, for the reasons described above, is inapplicable here, plaintiff's reliance on *In Re NSA Telecommunications Records Litigation* is unpersuasive and does not alter the conclusion reached here.[12]

In sum, when interpreted in light of traditional principles of statutory interpretation, the text of § 1806(f) makes clear that § 1806(f) procedures do not apply where, as here, the plaintiff has merely plausibly alleged that it has been the target of surveillance and has not yet adduced evidence establishing this fact of surveillance. Accordingly, it is not appropriate at this time to engage in *ex parte* and *in camera* review of the materials responsive to plaintiff's interrogatories or to those plaintiff describes in its motion to compel.

IV.

[12] It is also worth noting that despite the *In re NSA Telecommunications Records Litigation* court's determination that the plaintiffs there had sufficiently alleged their aggrieved person status, the court nonetheless declined to follow the mandatory § 1806(f) procedures. 595 F.Supp.2d at 1086-90. Specifically, the court ordered the government to produce responsive materials, but has yet to make a finding as to the lawfulness of any surveillance and has not provided the plaintiffs access to any discovery materials. *Id.*

Plaintiff also cites to *Jewel v. NSA*, a Northern District of California case in which the district court issued several orders, directing the government to produce materials for *ex parte* and *in camera* review. But the *Jewel* court appeared not to address the requisite showing of "aggrieved person" status, and as such, that case did not directly address the issues addressed here. Indeed, the *Jewel* court has not yet issued an order as to the lawfulness of any alleged surveillance in that case and has recently issued an order requesting additional briefing on how plaintiffs can "establish they may be aggrieved persons without access to [classified] information" and "the current legal standard for asserting standing in these circumstances." *Jewel v. NSA*, No. 08-cv-4373, at *1 (N.D. Cal. July 5, 2018). As such, it is clear that the *Jewel* court has not yet definitively resolved the issues addressed here.

Given that § 1806(f) procedures do not apply here, it is unnecessary to consider the question whether § 1806(f) displaces the state secrets privilege in situations in which § 1806(f) does apply. As such, the only remaining question is whether the government's invocation of the state secrets privilege defeats plaintiff's motion to compel.

A.

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

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

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

Albit, 848 F.3d at 311 (quoting *El-Masri*, 479 F.3d at 304).

With respect to the first step in this analysis, the Supreme Court has specified three procedural requirements for invocation of the state secrets privilege: (i) the state secrets privilege must be asserted by the United States government; it "can neither be claimed nor waived by a private party," (ii) "[t]here must be a formal claim of privilege, lodged by the head of the department which has control over the matter," and (iii) the department head's formal claim of the state secrets privilege must be made only "after actual personal consideration by that officer." *Reynolds*, 345 U.S. at 7-8 (footnotes omitted). If these procedural requirements are satisfied, the court may proceed to the second step of the analysis.

This second step of the analysis requires courts to "determine whether the information that the United States seeks to shield is a state secret, and thus privileged from disclosure." *El-Masri*, 479 F.3d at 304. In this respect, courts must "assure [themselves] that an appropriate balance is struck between protecting national security matters and preserving an open court system." *Albit*, 848 F.3d at 311-12 (quoting *Al-Haramain Islamic Found., Inc. v. Bush*, 507 F.3d 1190, 1203 (9th Cir. 2007)). That is, courts assessing a claim of state secrets privilege must simultaneously accord "utmost deference"[13] to the Executive Branch's assessment of the risk to national security posed by the disclosure of information while also "critically examin[ing] instances of [the privilege's] invocation" so as "not to accept at face value the government's claim or justification of privilege."[14]

The Supreme Court has balanced these competing concerns by requiring courts to determine "from all the circumstances of the case, [whether] there is a reasonable danger that compulsion of the evidence will expose . . . matters which, in the interest of national security,

---

[13] *Albit*, 848 F.3d at 312 (quoting *United States v. Nixon*, 418 U.S. 683, 710 (1974), *superseded by statute on other grounds as recognized by Bourjaily v. United States*, 483 U.S. 171, 177-79 (1987)).

[14] *Id.* at 312 (quoting *Al-Haramain*, 507 F.3d at 1203; *Ellsberg v. Mitchell*, 709 F.2d 51, 58 (D.C. Cir. 1983)).

should not be divulged.'" *Reynolds*, 345 U.S. at 10. The government bears the burden of satisfying "the reviewing court that the *Reynolds* reasonable-danger standard is met." *Albit*, 848 F.3d at 312 (quoting *El-Masri*, 479 F.3d at 305). In this regard, the Fourth Circuit has recognized that the explanation proffered by the department head who formally invokes the privilege is "frequently . . . sufficient to carry the Executive's burden." *Id.* (quoting *El-Masri*, 469 F.3d at 305). In the end, if the government carries its burden and shows that there is a reasonable danger that disclosure of information will expose matters that should not be divulged, "court[s] [are] obliged to honor the Executive's assertion of the privilege[.]" *Id.* (quoting *El-Masri*, 479 F.3d at 305).

If the procedural requirements for invocation of the state secrets privilege are satisfied and the court determines that the information sought to be disclosed is properly privileged, the final step in the analysis is to assess how the matter should proceed. Here, again, Fourth Circuit and Supreme Court precedent is clear: if the state secrets privilege has been successfully invoked, "the claim of privilege will be accepted without requiring further disclosure." *Id.* (quoting *Reynolds*, 345 U.S. at 9).

B.

With these principles in mind, it is appropriate now to consider the assertion of the state secrets privilege in this case. To begin with, the procedural requirements for invocation of the state secrets privilege have been satisfied.[15] Defendants, the NSA, ODNI, and the DOJ, are U.S. government agencies and thus can properly claim the state secrets privilege. The claim of privilege was lodged by Daniel Coats ("Coats"), the Director of National Intelligence ("DNI"), who is the head of the U.S. Intelligence Community and in this regard, is tasked with the protection of

[15] Indeed, Wikimedia does not appear to dispute this point.

intelligence sources and methods from unauthorized disclosure. *See* Coats Decl. ¶ 1.[16] Finally, Coats invoked the privilege formally after personally considering the nature of plaintiff's discovery requests and determining that disclosure of the information requested reasonably could be expected to cause exceptionally grave damage, and at the very least, serious damage, to U.S. national security. *See* Coats Decl. ¶¶ 6, 16, 24, 28, 32, 35, 39, 43. Accordingly, it is clear that defendants have satisfied the procedural requirements for invocation of the state secrets privilege.

The government has similarly satisfied its burden with respect to the second step of the state secrets privilege analysis as careful review of the public Coats declaration and the classified Barnes declaration reveals 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. Specifically, through public and classified declarations defendants have identified seven categories of information covered by plaintiff's discovery requests, including: (i) entities subject to Upstream surveillance activities, (ii) operational details of the Upstream collection process, (iii) locations at which Upstream surveillance is conducted, (iv) categories of Internet-based communications subject to Upstream surveillance activities, (v) the scope and scale on which Upstream surveillance is or has been conducted, (vi) NSA's cryptanalytic capabilities, and (vii) additional categories in contained in FISC opinions and submissions. Moreover, defendants have provided detailed descriptions, in more than 60 pages of classified declarations, explaining that disclosure of these categories of information would undermine ongoing intelligence operations, deprive the NSA of existing intelligence methods, and significantly, provide foreign adversaries with the tools necessary both to evade U.S. intelligence operations and to conduct their

[16]*See also* 50 U.S.C. § 3024(i)(1) (providing that "[t]he Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure.").

own operations against the United States and its allies. In sum, it is clear that there is a reasonable, and indeed likely, danger that disclosure of this information will expose matters which should not be divulged in the interest of national security, and as such, this information falls squarely within the ambit of the state secrets privilege. *See, e.g.*, *Albit*, 848 F.3d at 314 (concluding that "[t]here is little doubt that there is a reasonable danger that if information . . . regarding . . . the sources and methods used by the CIA [and] the targets of CIA intelligence collection and operations . . . were revealed, that disclosure would threaten the national security of the United States").[17]

In an attempt to avoid this conclusion, plaintiff contends that to acknowledge the fact that plaintiff has been subject to surveillance would not, in fact, threaten national security. This argument plainly fails because courts have concluded that where, as here, the information sought to be disclosed involves the identity of parties whose communications have been acquired, this information is properly privileged. *See* Al-*Haramain*, 507 F.3d at 1203-04 (finding that the fact of a plaintiff's surveillance by the NSA was covered by the state secrets privilege); *Halkin v. Helms*, 598 F.2d 1, 9 (D.C. Cir. 1978) (upholding assertion of state secrets privilege with respect to "the identity of particular individuals whose communications have been acquired").

Plaintiff contends that, contrary to surveillance of a particular individual with limited communications, plaintiff's communications are so ubiquitous that to reveal surveillance of its communications would not provide information regarding the structure of the Upstream surveillance program or its specific targets. Although this proposition may appear to have some force, courts have consistently recognized that "judicial intuition" about a proposition such as this

---

[17] *See also, e.g.*, *Sterling v. Tenet*, 416 F.3d 338, 342 (4th Cir. 2005) ("There is no question that information that would result in . . . disclosure of intelligence-gathering methods or capabilities . . . falls squarely within the definition of state secrets." (quoting *Molerio v. FBI*, 749 F.2d 815, 820-21 (D.C. Cir. 1984) (internal quotation marks omitted)); *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").

"is no substitute for documented risks and threats posed by the potential disclosure of national security information." *Al-Haramain*, 507 F.3d at 1203. And defendants have thoroughly documented those risks in the classified declaration here, 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 so doing, undermine the effectiveness of this intelligence method.

Finally, plaintiff argues that there cannot be a reasonable danger of undermining national security because much of the information plaintiff seeks is already contained in publicly-accessible documents. But importantly, the information disclosed in these public documents is plainly different from the information that plaintiff seeks. For example, plaintiff's requests for admissions 13 through 15 ask defendants to admit that the NSA is conducting Upstream surveillance via "multiple INTERNET BACKBONE CIRCUITS," "multiple international Internet link[s]," and "multiple INTERNET BACKBONE 'chokepoints.'" Plaintiff contends that these facts have already been acknowledged by the NSA, as reflected in the PCLOB Report and certain unclassified portions of FISC opinions. Specifically, plaintiff contends that the PCLOB report's reference to "circuits" suggests the NSA is conducting surveillance on more than one circuit. To be sure, the PCLOB report does use the term "circuits," but it does not do so to refer to the number of sites the NSA is monitoring. Instead, the PCLOB report uses the term "circuits" in the context of defining the "Internet backbone." Specifically, the PCLOB report explains that the "Internet backbone" consists of "circuits that are used to facilitate Internet communications[.]" PCLOB Rep. at 36. Similarly, the redacted FISC Opinion cited by plaintiff does not, as plaintiff contends, confirm that the NSA is monitoring multiple international Internet links; instead, the redacted October 3, 2011 FISC Opinion states 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 the NSA . . . ." 2011 WL 10945618, at *15 (FISC Oct. 3, 2011). Nothing in this statement confirms that the NSA is monitoring multiple internet links.[18] Ultimately, plaintiff's argument fails because although the government has declassified certain information about the Upstream surveillance program, the government has not yet released the precise information at issue here. Accordingly, this information is still properly subject to the state secrets privilege.

In sum, a careful review of defendants' public and classified declarations reveals (i) that defendants have satisfied the procedural requirements necessary to invoke the state secrets privilege and (ii) that the information sought to be protected qualifies as privileged under the state secrets doctrine. Given that defendants have satisfied the requirements of the state secrets privilege, "the claim of privilege will be accepted without requiring further disclosure." *Albit*, 848 F.3d at 31 (quoting *Reynolds*, 345 U.S. at 9). Accordingly, plaintiff's motion to compel must be denied.[19]

An appropriate Order will issue.

Alexandria, Virginia
August 20, 2018

/s/

T. S. Ellis, III
United States District Judge

[18] Plaintiff similarly argues that the fact that the NSA reviews the type of Internet communications in which plaintiff engages, namely HTTP and HTTPS Internet protocols, is available in the public record. But contrary to plaintiff's suggestion, the use of the general phrase "web activity" in an unclassified portion of the June 1, 2011 FISC Opinion does not confirm that the NSA is monitoring any specific Internet protocol, namely either HTTP or HTTPS.

[19] It is worth emphasizing the narrow scope of this decision, namely (i) that FISA § 1806 is not triggered in this case and that this provision and the associated FISA procedures do not operate here to displace the common law state secrets privilege and (ii) that the government has satisfied the well-settled procedural requirements necessary to invoke the privilege. Neither addressed nor resolved here is whether this long-ago judicially created privilege has, or should have, any continuing vitality today. That is not a question within the province of a district court.