STUART F. DELERY
Assistant Attorney General
JOSEPH H. HUNT
Director, Federal Programs Branch
ANTHONY J. COPPOLINO
Deputy Branch Director
JAMES J. GILLIGAN
Special Litigation Counsel
MARCIA BERMAN
Senior Trial Counsel
BRYAN DEARINGER
Trial Attorney
RODNEY PATTON
Trial Attorney
U.S. Department of Justice, Civil Division
20 Massachusetts Avenue, NW, Rm. 6102
Washington, D.C. 20001
Phone: (202) 514-3358; Fax: (202) 616-8470

Attorneys for the Government Defendants

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

CAROLYN JEWEL, *et al.*, Plaintiffs, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	Case No. C-08-4373-JSW
VIRGINIA SHUBERT, *et al.*, Plaintiffs, v. BARACK OBAMA, President of the United States, *et al.* Defendants.	Case No. C-07-0693-JSW **GOVERNMENT DEFENDANTS' REPLY ON THRESHOLD LEGAL ISSUES AS ORDERED BY THE COURT AT THE SEPTEMBER 27, 2013, STATUS CONFERENCE** No Hearing Scheduled Courtroom Judge Jeffrey S. White

TABLE OF CONTENTS

PAGE

INTRODUCTION

From the outset of this case, the central threshold issue has been whether litigation of Plaintiffs' claims, including their standing to bring those claims, may proceed without risking or requiring disclosures concerning U.S. intelligence-collection activities that would harm national security. In support of their assertion of the state secrets privilege in fall 2012, the Government Defendants demonstrated that litigating Plaintiffs' claims would plainly risk or require harmful disclosures of such information as whether particular individuals were targets of or subject to alleged National Security Agency (NSA) intelligence activities, and whether particular telecommunications carriers have assisted the NSA in conducting the challenged activities. In *Jewel v. NSA*, 2013 WL 3829405, at *6 (N.D. Cal. July 23, 2013), the Court determined that the Government had properly invoked the state secrets privilege because it showed that disclosure of the information it sought to protect would adversely impact national security—a conclusion unaffected, as the Court recognized, by its holding that the privilege is displaced in this case by the procedures for *ex parte* review of classified information set forth in section 106(f) of the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1806(f). *Id.* at *8-9, 15.

That concern has not abated, despite public disclosures and official declassification decisions about NSA intelligence-gathering activities since June 2013. As the Government explained in response to the threshold questions on which the Court has directed the instant briefing, *see* Transcript of Proceedings dated September 27, 2013 ("Tr.") at 6-7, while the Government has acknowledged the existence of these programs and some general information about their operation, the Director of National Intelligence ("DNI") has determined that disclosure of the specific information needed for Plaintiffs to establish whether the content of or metadata pertaining to their communications have been collected under these programs can still reasonably be expected to cause exceptionally grave damage to the national security of the United States. Government Defendants' Supplemental Brief on Threshold Legal Issues (ECF No. 167) ("Gov't Supp. Br.") at 11-14; Public Declaration of James R. Clapper, Director of National Intelligence (ECF No. 168) ("Public DNI Decl.") ¶ 2. That is the very information Plaintiffs require not only to establish their Article III standing, but also, as the Government has

shown, to establish that they are "aggrieved persons" as to whom § 1806(f)'s procedures apply. Gov't Supp. Br. at 9-10.[1] Thus, the question the Court directed to Plaintiffs at the September 2013 status conference remains at the core of the litigation—can the Court adjudicate Plaintiffs' standing, whether through § 1806(f) proceedings or otherwise, "without resulting in [the] impermissible damage to ongoing national security efforts" that the Supreme Court warned against in *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1149 n.4 (2013). Tr. at 6-7. As demonstrated herein, the answer to that question is unavoidably no.

Plaintiffs' response to the Court's four questions can be reduced to three essential propositions: (1) that § 1806(f) provides an appropriate mechanism not only by which to adjudicate the legality of electronic surveillance, but also by which to ascertain whether individuals such as Plaintiffs have been "aggrieved" by alleged unlawful surveillance in the first instance; (2) that *Amnesty International's* rejection of *ex parte* proceedings to adjudicate the existence of classified facts applies only where the court's adjudication would reveal the identities of "targets" of Government surveillance; and (3) that the disclosure of the classified information required to litigate Plaintiffs' claims poses no threat to national security because "evidence" establishing their claims is already in the public domain.

As discussed below, none of these arguments is tenable. First, Plaintiffs have misconstrued § 1806(f), which authorizes *ex parte* review of classified information to determine the lawfulness of electronic surveillance under FISA only where litigants have already shown, without resort to privileged national security information, that they were targets of or subject to the surveillance whose legality they contest. Second, as this Court recognized during the September 2013 status conference, the risks to national security posed by *in camera* proceedings that the Supreme Court identified in *Amnesty International* include not only the disclosure of the targets of Government surveillance, but also the disclosure of any protected information that

[1] While the Government Defendants acknowledge that the reasoning by which the Court concluded that § 1806(f) preempts application of the state secrets privilege to Plaintiffs' statutory claims would apply equally to Plaintiffs' constitutional claims, the Government Defendants continue respectfully to disagree with the Court's holding on this issue, and reserve their right to contest the Court's ruling on this issue as may later be necessary and appropriate, including through interlocutory appeal of any subsequent order or ruling that risks disclosure of information over which the Government continues to assert privilege.

could damage ongoing national security efforts. Finally, Plaintiffs cannot show that their own communications (or records thereof) have been subject to collection based on evidence in the public domain, and determination of the standing issue will still require classified information over which the Government continues to assert privilege. Thus, as the Supreme Court warned in *Amnesty International*, the Court cannot adjudicate Plaintiffs' standing, even by resort to *ex parte, in camera* proceedings, without risking disclosures of information that could place national security at risk—and that is so regardless of any public speculation about the still-classified details of NSA intelligence activities.

In sum, the Court's threshold inquiries go to whether *ex parte* proceedings under § 1806(f) can be safely and properly utilized to adjudicate Plaintiffs' standing without endangering national security. As set forth further below, the answer to that question is no, and the Court should not risk harm to national security by attempting to adjudicate Plaintiffs' standing (much less the merits of their claims) through proceedings under § 1806(f).

BACKGROUND

Following the Court's July 2013 decision that the Government's valid assertion of the state secrets privilege in this case is displaced as to Plaintiffs' statutory claims by FISA § 1806(f), the Court called for additional briefing on the following topics: (1) whether § 1806(f) also displaces the state secrets privilege as to Plaintiffs' constitutional claims; (2) whether the Court must follow § 1806(f)'s procedures in adjudicating the constitutional claims; (3) assuming § 1806(f) procedures may be used here, whether Plaintiffs can establish their standing without impermissible damage to national security; and (4) the impact of disclosures and declassification decisions by the Government since June 2013 on the Government's assessment of the risks to national security presented by this case. *See* Tr. at 6-7.

On December 20, 2013, the Government Defendants submitted their brief on the three issues (nos. 1, 2, and 4) that the Court directed them to address. The Government Defendants preserved their position that § 1806(f) does not displace the state secrets privilege, but otherwise did not contest that the Court's theory of displacement would apply equally to Plaintiffs' constitutional claims as to their statutory causes of action. The Government explained, however,

that even if § 1806(f) displaces the privilege "in cases within [the statute's] reach," *Jewel*, 2013 WL 3829405, at *9, § 1806(f) applies by its own terms only where an individual can first demonstrate that he or she is an "aggrieved person" under that provision, which FISA defines to mean a person who has been the "target of" or "whose communications or activities were subject to" "electronic surveillance." 50 U.S.C. § 1801(k). *See* Gov't Supp. Br. at 7-10. The Government then set forth the impact of recent declassification decisions on this case, explaining that the existence of surveillance activities authorized by then-President Bush after the September 11, 2001, terrorist attacks (known collectively as the President's Surveillance Program ("PSP")), later transitioned to authority under FISA, has now been declassified, but that certain information concerning those activities, including most notably whether particular individuals, including Plaintiffs, have been subject to NSA intelligence activities, and whether any telecommunications carriers have provided assistance to the NSA in connection with any intelligence activities, remains properly protected from disclosure. *Id.* at 11.

As set forth below, Plaintiffs' response to the Court's questions (*see* ECF No. 177) fails to demonstrate how their claims can proceed without risk of further harm to national security.

DISCUSSION

A. Litigation of Plaintiffs' Standing Will Risk or Require Harmful Disclosures of Still Classified Information About NSA Intelligence Programs Regardless of Whether the Litigation Proceeds Under § 1806(f) or Not.

Plaintiffs' own vision for the litigation of this case demonstrates that the threshold question of Plaintiffs' standing to maintain this action cannot be litigated without risking or requiring disclosures of privileged state secrets that could endanger national security.

In fall 2012, the Government asserted the state secrets privilege (as well as other statutory privileges) over (1) information tending to confirm or deny whether Plaintiffs have been subject to any alleged NSA intelligence activities at issue in this case, and (2) any other information about the scope and operation of the alleged NSA intelligence activities to litigate Plaintiffs' claims, including information that may tend to confirm or deny whether any particular telecommunications company has provided assistance to the NSA in connection with any alleged

activity. *See* Gov't Defs.' Second Mot. To Dismiss and for Summary Judgment and Opp. to Pls.' Mot. for Partial Summ. Judg. (ECF No. 102) at 20-21.

The Government demonstrated in public and classified declarations by the DNI and the NSA that disclosure of the privileged information reasonably could be expected to cause exceptionally grave damage to national security. The DNI explained, for example, that disclosing whether specific individuals actually were targets of or subject to NSA intelligence-collection activities would reveal who is of investigative interest to the Government (helping such persons to evade surveillance), or who is not—thereby revealing the scope of intelligence activities as well as the existence of secure channels for terrorist operatives to communicate. *See id.* at 21. The DNI also demonstrated that disclosing whether particular telecommunications companies assisted with the alleged NSA intelligence activities could also be expected to cause exceptionally grave damage to national security by, *inter alia*, revealing to foreign adversaries which channels of communication may or may not be secure. *See id.* at 23. Upon review of the Government's submissions, the Court concluded that the Government had properly invoked the state secrets privilege "with regard to significant evidence tending to confirm or negate the factual allegations in Plaintiffs' complaints," notwithstanding "the multiple public disclosures of information regarding" the challenged programs. *Jewel*, 2013 WL 3829405, at *6-7.

These concerns remain just as acute today, despite the disclosures and declassification of some information over the past several months concerning the existence of, and limited information about, the challenged intelligence activities. As the Government Defendants have explained, Gov't Supp. Br. at 3, 11, the Government is no longer asserting the state secrets privilege, or the statutory privilege under 50 U.S.C. § 3024(i)(1), over the existence of the presidentially authorized NSA intelligence activities, later transitioned to authority under FISA, that are implicated by Plaintiffs' allegations. These activities included the collection of (1) the contents of certain international communications, involving persons reasonably believed to be agents of al Qai'da or its affiliated organizations, and (2) bulk telephony and Internet non-content communications information (referred to as "metadata"). But the disclosure of the additional information necessary to establish Plaintiffs' standing—and any determination by the

Court with respect to standing—still reasonably could be expected to cause exceptionally grave damage to national security, beyond what has already resulted from the unauthorized disclosures that have occurred since June 2013, by revealing information concerning targets or subjects of NSA intelligence activities, the scope and operational details of those activities, and the identities of telecommunications service providers that have assisted in those activities. Public DNI Decl. ¶¶ 2, 9-11, 19, 33-45; *see also* Unclassified Declaration of Frances J. Fleisch, National Security Agency (ECF No. 169) ("Public NSA Decl.") ¶¶ 21, 35-39, 45, 48.[2] Therefore, the DNI, supported by the NSA, has determined that it remains necessary to protect this still-classified information. Public DNI Decl. ¶¶ 5, 9, 11; Public NSA Decl. ¶¶ 6.

Plaintiffs' proposals for avoiding these risks would actually put the case on a collision course with the very harms they purport to avoid. Plaintiffs maintain that adopting their proposed "carefully staged discovery plan to separate public evidence from national security evidence" will insulate privileged information from disclosure. Pls.' Resp. (ECF No. 177) at 7. But the plan itself demonstrates the futility of such efforts.[3] Plaintiffs seek to take discovery,

[2] The Government has officially declassified an unlawfully disclosed and now expired order of the Foreign Intelligence Surveillance Court issued in April 2013, directing Verizon Business Network Services (a separate business entity from Verizon Wireless, *see United States ex rel Shea v. Verizon Bus. Network Servs., Inc.*, 904 F. Supp. 2d 28, 30 (D.D.C. 2012)) to produce telephony metadata to the NSA. Otherwise, the Government has not acknowledged, and continues to protect, the identities of companies that have participated at any time in the NSA's bulk telephony metadata program, and any other FISC- or presidentially authorized intelligence activities. Public DNI Decl. ¶¶ 42-44; Public NSA Decl. ¶¶ 21, 44-45.

[3] Plaintiffs suggest that the Court can defer ruling on the threshold legal issues until after the parties have implemented their proposed discovery plan. Pls.' Resp. at 7. The Court correctly rejected this approach at the September 2013 status conference. Tr. at 8. Even though the Court held that § 1806(f) preempts the state secrets privilege, *see Jewel v. NSA*, 2013 WL 3829405, at *7-9 (N.D. Cal. July 23, 2013), it also recognized that "the potential risk to national security may still be too great to pursue confirmation of … facts relating to the scope of the alleged government Program." *Id.* at *15. The time to address that concern is now, as reflected by the question the Court directed Plaintiffs to address. *See Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1083 (9th Cir. 2010) (holding that issue of whether harm to national security would result from proceeding in litigation should properly be addressed before further proceedings in the case); *see also Jewel*, 2013 WL 3829405, at *5 (same). Specifically, the Court must determine now whether Plaintiffs can establish their standing without reliance on privileged evidence, or, "even if the [standing issues] might theoretically be [addressed] without relying on privileged evidence," the Court must determine whether "it may be impossible to proceed with the litigation because—privileged evidence being inseparable from non-privileged information that will be necessary to the claims or defenses—litigating the case to a judgment on the merits would present an unacceptable risk of disclosing state secrets." *Jeppesen*, 614 F.3d at 1083; *Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998) ("recogniz[ing] the inherent limitations in trying to separate classified and unclassified information").

inter alia, into supposed carrier assistance by inspecting AT&T facilities allegedly involved in surveillance activities, by deposing telecommunications carrier executives about their allegations, and also questioning numerous current and former top-level national security officials about classified NSA activities. *See* Declaration of Cindy Cohn Pursuant to Fed. R. Civ. P. 56(d), (ECF No. 114) ¶¶ 7, 13-19; *see, e.g.*, *id*. ¶ 13 ("Plaintiffs would seek discovery regarding the fact of the carriers' interception and disclosure of the communications and communications records of [their] customers, including those of the named Plaintiffs and class members."). This is information at the heart of the Government's recently re-asserted privilege.

Plaintiffs also anticipate that if the Government believes a discovery request or deposition question calls for classified information, the Attorney General will personally submit an affidavit invoking *ex parte* review under § 1806(f), after which "Plaintiffs will then decide . . . whether to proceed under section 1806(f)." Joint Case Management Statement and [Proposed] Order, at 18-20 (ECF No. 159). The inherent flaws in this plan should be obvious. Above and beyond the burdens of deposing senior Government officials, and of submitting affidavits by the Attorney General in response to multiple rounds of discovery requests, attempting to draw lines between privileged and non-privileged information during the discovery process, particularly during real-time interrogation of deposition witnesses, itself risks harmful disclosures. *See Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1088 (9th Cir. 2010) (and cases cited therein) (noting dangers of permitting cross-examination of witnesses with knowledge of relevant state secrets where privileged and non-privileged information are intertwined); *El-Masri v. United States*, 479 F.3d 296, 307 (4th Cir. 2007) (same). Plaintiffs' discovery plan would require the parties to "play with fire and chance" the "inadvertent" or "mistaken" disclosure of classified information at every turn, *Sterling v. Tenet*, 416 F.3d 338, 344 (4th Cir. 2005), all for the putative purpose of determining Plaintiffs' standing *without* harm to national security.

The same is true, moreover, of the process Plaintiffs envision after invocation of § 1806(f), whereby classified evidence sought in discovery but withheld by the Government, including whether the contents of or metadata pertaining to a their communications have been collected by the NSA, would be turned over to the Court for *in camera* review to resolve the

standing issue. Pls.' Resp. at 7. Proceeding in that fashion would also risk the very concern identified by the Supreme Court in *Amnesty International*, 133 S. Ct. at 1149 n.4, because under those circumstances the court's "postdisclosure decision about whether to dismiss the suit for lack of standing would surely signal," *id.*, whether or not Plaintiffs' communications, or metadata pertaining to their communications, have been or may be collected by the NSA—the precise information that *in camera* review of the evidence was intended to protect.

By the same token, if the Government Defendants, pursuant to § 1806(f), present still-classified information to the Court regarding the identities of carriers that have participated in these programs, so as to avoid disclosure of this information in discovery, the path that Plaintiffs would have this case follow once again leads headlong to the risks that *Amnesty International* admonishes courts to avoid. Plaintiffs' framing of the standing issue turns on whether their carriers (AT&T in the *Jewel* case and Verizon in the *Shubert* litigation), assisted the NSA in conducting the challenged intelligence programs, and any decision by the Court that the Plaintiffs do or do not have standing to maintain this lawsuit would be tantamount to disclosing that evidence submitted by the Government establishes that AT&T (or Verizon) has or has not participated in NSA intelligence-gathering activities, with the risk of grave damage to national security that would ensue. Public DNI Decl. ¶¶ 2, 9-11, 19, 42-44; Public NSA Decl. ¶¶ 6, 21, 35, 48. *See also* Classified DNI and NSA Declarations. This is an unworkable plan.

In short, execution of Plaintiffs' own proposals for litigation of the standing issue would court the very risks to national security against which the Ninth Circuit, other courts of appeals, and, most recently, the Supreme Court in *Amnesty International* have consistently warned. The answer to the Court's third threshold question is that Plaintiffs cannot establish their standing without risking damage to ongoing national security efforts, Tr. at 6-7, and in the interests of national security, the attempt should not be made.[4]

[4] Because use of § 1806(f)'s procedures to determine whether Plaintiffs have standing would inherently risk or require the disclosure of information subject to the state secrets privilege, the Court should not risk abrogation of the privilege, directly or indirectly, without first providing the Government with an opportunity for appellate review of whether that adjudication would be proper. *See In re Copley Press, Inc.*, 518 F.3d 1022, 1025 (9th Cir. 2008) ("Secrecy is a one-way street; Once information is published [or disclosed], it cannot be made secret again," and thus an order of disclosure is "'effectively unreviewable on appeal from a final judgment'" (quoting *Coopers & Lybrand v. Livesay*, 437 U.S. 463, 468 (1978)). Indeed, § 1806

B. The Provisions of § 1806(f) Apply Only if Plaintiffs Can First Prove That They Are "Aggrieved Persons" Challenging "Electronic Surveillance."

Pivotal to Plaintiffs' "carefully staged" plan for litigating their standing is the availability under § 1806(f) of *ex parte, in camera* review of still-classified, privileged information needed to decide the question. *See* Pls.' Resp. at 7-8. But even assuming *arguendo* that § 1806(f) displaces the state secrets privilege in this case, it operates as a mechanism, invoked by the Attorney General, allowing a court to conduct *ex parte, in camera* review of classified information to determine the lawfulness of electronic surveillance challenged by persons who it has already been shown were targets of or subject to such surveillance. *See* Gov't Defs.' Supp. Br. at 7-11. *Ex parte* review under § 1806(f) cannot be used to determine *whether* Plaintiffs are aggrieved persons who have been subject to electronic surveillance in the first instance—and thus whether they have standing here—because to do so would contradict the plain language of the statute, its legislative history, and its consistent application by the courts.

By its terms, § 1806(f) provides a mechanism whereby, "whenever any motion or request is made by an *aggrieved person* … to discover or obtain … materials relating to electronic surveillance" under FISA, the Attorney General may attest that "disclosure … would harm the national security of the United States," whereupon the court "may review in camera … [the] materials relating to the surveillance as may be necessary to determine whether the surveillance of the *aggrieved person* was lawfully authorized and conducted." 50 U.S.C. § 1806(f) (emphasis added). FISA defines an "aggrieved person" as a person "who is the target of … or whose communications or activities were subject to electronic surveillance." *Id*. § 1806(k). Thus, the only determination for which the Court is authorized to conduct *ex parte, in camera* review of classified information under § 1806(f) is "whether the [challenged] surveillance … was lawfully authorized and conducted." Whether the movant is an "aggrieved person" who was a target or subject of the surveillance is an antecedent question that must be determined as a pre-requisite to, not by means of, *ex parte* proceedings under the statute. In short, nothing in the text of § 1806(f)

---

itself recognizes that an appeal may be necessary *before* disclosures of information concerning surveillance activities are compelled. *See* 50 U.S.C. § 1806(h) ("orders of the United States district court requiring review or granting disclosure of . . . materials relating to a surveillance [under § 1806(f)] shall be final orders . . . .").

indicates that individuals can trigger *ex parte, in camera* review by seeking to discover whether they have been subjects of alleged surveillance.[5]

This conclusion not only follows from the statute's plain language, but is also firmly supported by the legislative history. Congress crafted the *ex parte, in camera* procedure of § 1806(f) to satisfy the requirements of *Alderman v. United States*, 394 U.S. 165, 167-68, 170 n.3, 182-87 (1969) (holding that a criminal defendant whose communications the Government acknowledged intercepting was entitled to transcripts of the recorded conversations to determine if any evidence used against him was tainted by unlawful surveillance), while at the same time avoiding harmful disclosures of foreign intelligence information by allowing the Attorney General to seek *ex parte, in camera* review of suppression motions brought by "aggrieved persons." *See* S. Rep. 95-701, at 65. In so doing, Congress explained that the term "aggrieved person" was meant to be "coextensive [with], but no broader than, those persons who have standing to raise claims under the Fourth Amendment with respect to electronic surveillance, and therefore that litigants who cannot establish their status as "aggrieved persons" do "not have standing" under "any" of FISA's provisions." H.R. Rep. No. 95-1283, 66, 89-90 (1978). *See also Director, Office of Workers' Comp. Programs v. Newport News Shipbuilding & Dry Dock Co.*, 514 U.S. 122, 126 (1995) ("aggrieved" is a well-known term of art used "to designate those who have standing"). As even Plaintiffs acknowledge, the term "aggrieved person" was meant "to exclude 'persons, *not* parties to a communication, who may be mentioned or talked about by others,' because Congress had 'no intent to create a statutory right in such persons.'" Pls.' Resp. at 8 (quoting H.R. Rep. No. 95-1283 at 66).

[5] In response to the Government Defendants' observation that "not a single court applying § 1806(f) has ever granted an aggrieved person access to underlying surveillance information following *in camera* proceedings," Gov't Defs.' Supp. Br. at 10 n.6, Plaintiffs refer to a recent district court decision, issued after the Government Defendants' supplemental brief was filed, in which the court, while acknowledging that "no court has ever allowed disclosure of FISA materials to the defense," directed disclosure of FISA surveillance materials (in redacted form, if necessary) to a criminal defendant's counsel who asserted that he already held the appropriate security clearance. *See* Pls.' Br. at 9 n.4, citing *United States v. Daoud*, 1:12-cr-00723 (N.D. Ill.), ECF No. 92, at 4-5. The Government has appealed that decision to the Seventh Circuit. *Id.*, ECF No. 97. Moreover, *Daoud* is not precedent for the procedure Plaintiffs envision in this case, as in *Daoud* the Government had already given the defendant notice of its intent to use FISA evidence against him, *see id.*, ECF No. 9, so there was no question that he was an "aggrieved person" under § 1806(f).

Also instructive is the Senate Intelligence Committee's discussion of 18 U.S.C. § 3504. S. Rep. No. 95-701 at 63. Under § 3504, the Government must affirm or deny the occurrence of surveillance when a criminal defendant who "claim[s]" to be aggrieved by allegedly unlawful surveillance challenges the admissibility of evidence he believes was derived therefrom. 18 U.S.C. § 3504(a)(1); *see United States v. Shelton*, 30 F.3d 702, 707 (6th Cir. 1994) ("Section 3504 comes into play only on a claim that evidence is inadmissible."). The Senate Intelligence Committee report observes that the "most common circumstance" in which a suppression motion might be brought under § 1806(f) would be "*after* a defendant queries the Government under 18 U.S.C. § 3504 and discovers that he has been intercepted by electronic surveillance …." S. Rep. No. 95-701, at 63 (emphasis added). Thus, Congress contemplated that it will be known *whether* a party is an aggrieved person who has been subject to surveillance *prior* to a court determining the lawfulness of the surveillance through *ex parte* proceedings under § 1806(f).

Consistent with the text of § 1806(f) and its surrounding legislative history, courts have consistently construed the term "aggrieved person" to mean that only litigants who can establish that their communications were subject to electronic surveillance may proceed to challenge the lawfulness of the surveillance, *see, e.g., United States v. Ott*, 827 F.2d 473, 475 n.1 (9th Cir. 1987) ("Because Ott's communications were subject to surveillance, he is an aggrieved person with standing to bring a motion to suppress pursuant to section 1806(e)"); *United States v. Cavanaugh*, 807 F.2d 787, 789 (9th Cir. 1987) ("Appellant was a party to an intercepted communication, and the government concedes he is an 'aggrieved person' within the meaning of the statute. The appellant has standing to challenge the government's compliance with [the FISA's statutory requirements]"). In contrast, litigants who cannot establish that they are aggrieved persons cannot proceed under § 1806(f). *See, e.g.*, *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); *In re Motion for Release of Court Records*, 526 F. Supp. 2d 484, 487 (F.I.S.C. 2007) ("The ACLU comes to [the FISA] Court claiming a right of access as a member of the public, not as an aggrieved person who has received the statutory notification.").[6]

[6] *See also United States v. Damrah*, 412 F.3d 618, 622-24 (6th Cir. 2005) (§ 1806(f) applied where Government admitted audio tapes of FISA surveillance during trial); *In re Sealed*

Plaintiffs cite nothing in the text or legislative history of § 1806(f), or in the case law, to support their contrary position that *ex parte* proceedings under § 1806(f) are available to determine whether an individual is an aggrieved person in the first place. Instead they attempt to denigrate the Government Defendants' construction of the statute as an "essentially circular, and nonsensical, argument that plaintiffs cannot use § 1806(f) proceedings in proving their case unless they have already proven their case using non-secret evidence." Pls.' Br. at 7-8, citing *In re NSA Telecomm. Records. Liigt. (Al-Haramain),* 595 F. Supp. 2d 1077, 1085 (N.D. Cal. 2009). The Government Defendants have argued nothing of the sort. Rather, they have observed only that the statute requires Plaintiffs to establish that they are aggrieved persons—not to prove the *merits* of their claims—before they can invoke the procedures under § 1806(f) that can lead to *ex parte* review of classified information.[7] Gov't Defs.' Supp. Br. at 7-10. That understanding of the statute is consistent with the Ninth Circuit's observation in *Al-Haramain Islamic Found., Inc. v. Bush*, 507 F.3d 1190, 1204 (9th Cir. 2007), that "[a]lthough FISA permits district court judges to conduct an *in camera* review of information relating to electronic surveillance, there are detailed procedural safeguards"—and here the court cited § 1806(f) specifically—"that must be satisfied *before* such review can be conducted" (emphasis added). One of those "procedural safeguards" is that Plaintiffs must be aggrieved persons for § 1806(f) to apply.[8]

Case, 310 F.3d 717, 741 (F.I.S.C. Rev. 2002) ("FISA does not require notice to a person whose communications were intercepted unless the government intends to enter into evidence or otherwise use or disclose such communications in a trial or other enumerated official proceedings."); *United States v. Hamide*, 914 F.2d 1147, 1148-50 & n.2 (9th Cir. 1990) (in deportation proceeding where Government admitted FISA-authorized surveillance occurred, court determined lawfulness of acknowledged surveillance under § 1806(f) procedure); *United States v. Duggan*, 743 F.2d 59, 67-68 (2d Cir. 1984) (Government provided notice of use of surveillance evidence under § 1806(c) and § 1806(f) applied in response to motion to suppress).

[7] Plaintiffs expend a great deal of effort (Pls.' Br. at 9-10) rebutting what they take to be "the government's apparent suggestion" that the Attorney General may, in his discretion, "withhold[] evidence [and] block the Court from deciding the legality of the surveillance." Pls.' Br. at 9. The Government Defendants did not make this argument either. We merely detailed, in the passage to which Plaintiffs refer, how the statutory mechanism (as the Court has construed it) would work: the submission of a motion by an aggrieved person, followed by a decision by the Attorney General whether to invoke the statutory mechanism, and then the Court's *ex parte, in camera* review of the classified information. *See* Gov't Defs.' Supp. Br. at 10.

[8] Plaintiffs also contend that "18 U.S.C. § 2712 further reinforces the conclusion that section 1806(f) controls here and that the government must follow its procedures if it refuses discovery on national security grounds." Pls.' Br. at 10. But that argument is to no avail. Section 2712(a) also requires that the person seeking to use § 1806(f) in such a civil action be

Plaintiffs also argue that the Court should import into § 1806(f) the "party aggrieved" standard of 18 U.S.C. § 3504. Pls.' Resp. at 8 & n.3. But that suggestion should be rejected because the two statutes perform distinct functions. As discussed *supra*, at 11, § 3504(a)(1) allows a person against whom the government is offering evidence to "claim" that the evidence is inadmissible as the "product of an unlawful act" (such as unauthorized electronic surveillance) and thereupon require the Government to "affirm or deny the occurrence" of the "alleged unlawful act." 18 U.S.C. § 3504(a)(1). The Ninth Circuit has stated that a person "claim[ing]" that he was a subject of the "alleged" surveillance need only make a "preliminary showing" to that effect, *In re Grand Jury Proceedings (Garrett)*, 773 F.2d 1071, 1072 (9th Cir. 1985) (per curiam), that is "sufficiently concrete and specific" to require a response by the Government, *United States v. Waters*, 627 F.3d 345, 364 (9th Cir. 2010), because the statute's very purpose is to determine *whether* the alleged surveillance of the claimant occurred. *See* 18 U.S.C. § 3504(a)(1); S. Rep. No. 95-701, at 63; *United States v. Vielguth*, 502 F.2d 1257, 1259-62 (9th Cir. 1974). Section 1806(f) contains no similar provision. Rather, in a § 1806(f) proceeding, the statutory language *presupposes* that surveillance has occurred, because the only determination a reviewing court is authorized to make is "whether the surveillance" of a person "was lawfully authorized and conducted," not whether surveillance of the individual occurred in the first place. 50 U.S.C. § 1806(f); *see also* S. Rep. No. 95-701, at 63. Congress was well aware of § 3504 when it enacted § 1806, *see supra* at 11, citing S. Rep. No. 95-701, at 63, and could have included language, like that used in § 3504, that might require the Government to affirm or deny that surveillance had occurred upon a "claim" by an aggrieved person that the "alleged" surveillance had occurred. But Congress did not do so.[9]

"aggrieved" (rather than claim to be aggrieved). *See* 18 U.S.C. § 2712(a). Additionally, Section 2712(b)(4), on which Plaintiffs rely, states only that § 1806(f) would apply to the materials "governed by" 1806(f), which, of course, brings the analysis back to *how* § 1806(f) operates and whether or not Plaintiffs may proceed without first establishing that they are aggrieved persons so as to come within the meaning of the statute.

[9] Plaintiffs cite Judge Walker's decision for the Court in *Al-Haramain* as holding that litigants need not submit proof that they have been subject to surveillance—only allegations—to establish their status as "aggrieved person[s]" under § 1806(f). Pls.' Resp. at 8 & n.3, citing 595 F. Supp. 2d at 1085. On this point, we respectfully submit that the Court in *Al-Haramain* erred. Judge Walker relied on the Ninth Circuit's decision *United States v. Alter*, 482 F.2d 1016 (9th Cir. 1973) for the proposition that, under 18 U.S.C. § 3504, "*proof* of plaintiffs' claims [of

As discussed above, in circumstances such as those presented here, a litigant's standing cannot be adjudicated based on *ex parte* review of privileged state secrets without endangering national security. Consistent, however, with the purpose of § 1806(f) to protect against improper disclosures of national security information, the terms of the statute do not allow parties to invoke its procedures as a mechanism for litigating whether they have been subject to surveillance, but only as a means of determining whether surveillance of persons who have already established their aggrieved person status was lawful.

C. Litigating Plaintiffs' Standing by Way of *Ex Parte* Proceedings Under § 1806(f) Would Endanger National Security in Exactly the Manner Condemned by the Supreme Court in *Amnesty International.*

At the September 2013 status conference, the Court directed Plaintiffs to address the third of its four threshold questions, whether they can "establish [their] standing to sue *without resulting in impermissible damage to ongoing national security efforts.*" Tr. at 6 (emphasis added). Instead of answering this question, Plaintiffs assert that the "Court ask[ed]" a different question more to their liking, "whether a ruling [on their standing] … [would] *reveal who[m] the government has targeted for surveillance*," and pronounce that "no such risk is present here." Pls.' Resp. at 10 (emphasis added). Notwithstanding their unilateral attempt to re-formulate the question the Court instructed them to answer, Plaintiffs fail to show that the Court can adjudicate their standing through *ex parte* review of classified evidence under § 1806(f) without running afoul of the Supreme Court's admonition in *Amnesty International* that courts should not engage

---

surveillance] is not necessary" where "[t]he court has determined that the allegations 'are sufficiently definite, specific, detailed, and nonconjectural, to enable the court to conclude that a substantial claim is presented.'" 595 F. Supp. 2d at 1085, citing *Alter*, 482 F.2d at 1025. First, *Alter* (like all cases applying § 3504) involved the actual *use* of surveillance evidence against a person—a circumstance not presented here. Second, Judge Walker erroneously imported the standard for a preliminary showing under § 3504 to determine the plaintiffs' status as "aggrieved persons" under § 1806(f), where the FISA contains no such provision. Third, Judge Walker was mistaken in holding that even § 3504's requirement could be satisfied by mere allegations. As *Alter* and its progeny make clear, even under § 3504 a litigant claiming "party aggrieved" status must submit "affidavit(s) or other evidence" that reveal "specific facts" supporting the claim that the individual in question was subjected to the alleged surveillance. 482 F.2d at 1026; *see also Waters*, 627 F.3d at 364 (preliminary showing of "party aggrieved" status under § 3504 must be "sufficiently concrete and specific"); *United States v. See*, 505 F.2d 845, 856 (9th Cir. 1974). (As discussed *infra*, at 20-21, Plaintiffs have made no such showing in this litigation.) Neither § 3504 nor *Alter* sheds any light on how § 1806(f) operates.

in *ex parte* adjudication of litigants' standing where a court's decision would itself result in harmful disclosures of national security information. 133 S. Ct. at 1149 n.4.

Plaintiffs' principal argument on this issue is that *Amnesty International's* proscription is not implicated under the circumstances of this case, because any finding that they have been "subjected to untargeted mass surveillance does *not* 'signal to [them] whether [their] name[s are] on the list of surveillance targets.'" Pls.' Resp. at 12, quoting *id.* Plaintiffs therefore conclude that what they construe to be the Supreme Court's "fundamental concern—that litigation of a plaintiff's targeted-surveillance claim would unavoidably reveal who[m] the government is targeting for surveillance—is entirely absent here." *Id.* at 13. This argument is meritless.

Amnesty International spoke of the risk of revealing targets of surveillance because, on the facts of the case before the Court, that was the information that adjudicating a litigant's standing could disclose. But what manifestly concerned the Court was not the specific type of national security information that would be revealed, but the concern that any decision regarding a party's standing that is based on a court's *ex parte, in camera,* review of classified information would necessarily disclose the very information that the *ex parte* proceeding was meant to conceal.[10] The notion that the Supreme Court's concern in *Amnesty International* was limited to one type of intelligence information—"targets"—but not other classified information is simply unsupported and illogical. At bottom, the concern is the same as that confronted in cases concerning all manner of state secrets, in which the courts "are precluded from explaining precisely which matters the privilege covers lest [they] jeopardize the secrets [they] are bound to protect." *Jeppesen,* 614 F.3d at 1073-74, 1086, 1090 (upholding assertion of privilege over information that would tend to confirm or deny whether the defendant corporation or any foreign government assisted the CIA in conducting intelligence activities); *Jewel,* 2013 WL 3829405, at *6-7. This Court recognized as much when, citing *Amnesty International,* it instructed

[10] Contrary to Plaintiffs' arguments, this concern applies with equal force to disclosures of classified information about "past and ongoing surveillance," Pls.' Br. at 11, that could result from statutorily authorized *ex parte, in camera* proceedings, and not just the "hypothetical" proceeding referenced in *Amnesty International*. Pls.' Br. at 13-14.

Plaintiffs to explain how they can establish their standing, not simply without revealing targets of surveillance, but, more broadly, without endangering national security at all. Tr. at 6.

To conclude otherwise as Plaintiffs suggest would place national security at risk. For example, throughout this litigation Plaintiffs have argued that it would be sufficient to prove that the NSA has collected information pertaining to their communications—and thus to establish their standing—if they can prove that their telecommunications companies—AT&T and Verizon—have assisted the NSA in conducting the intelligence-gathering activities that Plaintiffs challenge here. *See, e.g.*, Pls.' Resp. at 18-19. But adjudicating Plaintiffs' standing on this basis, even if evidence concerning particular companies' participation were reviewed by the Court *ex parte*, would just as surely reveal whether specific companies have assisted in particular NSA programs as *ex parte* litigation of the standing issue in *Amnesty International* would have revealed the targets of Government surveillance—and at the same risk of exceptionally grave damage to national security. *Supra* at 5-6; Public DNI Decl. ¶¶ 2, 9-11, 19, 42-44; Public NSA Decl. ¶¶ 6, 21, 35, 48. There is no basis to suggest that the concerns underlying the Supreme Court's admonition in *Amnesty International* do not apply equally to this situation

Moreover, Plaintiffs' contention that the concern identified in *Amnesty International* does not apply here fails even on its own terms. Notwithstanding their repeated assertions that they are challenging a program of "untargeted mass surveillance," *e.g.*, Pls.' Resp. at 12, insofar as they purport to challenge NSA surveillance of communications content it remains the case that demonstrating their standing will require them to show that the contents of *their* communications have been collected. Thus, *ex parte* adjudication of litigants' standing to challenge the content collection alleged here would just as easily allow a target "to determine whether he is currently under U.S. surveillance" as would the *in camera* proceedings suggested by the plaintiffs, and rejected by the Court, in *Amnesty International*, 133 S. Ct. at 1149 n.4. Similarly, *ex parte* adjudication of whether records of Plaintiffs' communications have been subject to collection under the NSA's bulk telephony and Internet metadata programs would provide our adversaries with information about the specific scope of those activities, thus alerting them to which

channels of information are and are not secure for communication. *See supra* at 5-6; Public DNI Decl. ¶¶ 2, 9-11, 19, 33-45; Public NSA Decl. ¶¶ 21, 35-48.

Plaintiffs also argue that the Court must accept this potential risk to national security because it was ordained by Congress when it enacted § 1806(f). *See* Pls.' Resp. at 13 ("Congress has already weighed the balance between national security and the rule of law and has found that claims of unlawful surveillance should go forward … under the protective procedures of section 1806(f)"). In other words, according to Plaintiffs, Congress intended that courts engage in *ex parte* adjudication of litigants' standing in cases challenging electronic surveillance under FISA even where doing so would result in disclosures of privileged national security information that can reasonably be expected "to cause exceptionally grave damage to the national security of the United States." *See* Public DNI Decl. ¶ 17. But that result does not reflect the will of Congress; it is solely the consequence of Plaintiffs' textually unsupportable reading of § 1806(f) as authorizing *ex parte* review of classified evidence to determine whether a party is an "aggrieved person" who has been subject to surveillance.

Properly construed, § 1806(f) "ensures adequate protection of national security interests," as Congress intended. H.R. Conf. Rep. No. 95-1720, at 32. But when invoked, as here, for the purpose, unintended by Congress, of establishing whether litigants are "aggrieved persons" who were subject to surveillance, it engenders risks to national security that *Amnesty International* reminds courts they must avoid. This concern, as the Ninth Circuit anticipated, "doom[s]" Plaintiffs' efforts to establish their standing. *Jewel v. NSA*, 673 F.3d 902, 911 (9th Cir. 2011).

D. Notwithstanding the Declassification of Information About NSA Intelligence Programs Since June 2013, Plaintiffs' Standing Cannot Be Litigated Without Risking Grave Damage to National Security.

Finally, Plaintiffs contend that official and unofficial disclosures about NSA intelligence activities "confirm that plaintiffs' claims may be litigated without endangering national security," thus obviating the concerns the Supreme Court raised in *Amnesty International*, because the evidence "establishing plaintiffs' claims," including AT&T's alleged participation in "the surveillance," is already in the public domain. Pls.' Resp. at 14-16, 18-19; *see also id*. at 14-15. This contention can be taken to mean either that Plaintiffs believe they have no need to

rely on classified national security information over which the DNI has asserted privilege in order to litigate their claims, or that compelled disclosure (or *ex parte* review) of this information poses no risk to national security because the information has already been publicly disclosed. Either way, the argument fails.

First, Plaintiffs point to the fact that the Government has now officially acknowledged the *existence* of the NSA's activities involving the targeted collection of the contents of suspected terrorist communications, and the bulk collection of telephony and Internet metadata. Pls.' Resp. at 16-17. The official acknowledgement of these programs is of no assistance to Plaintiffs. It is not enough for Plaintiffs to prove the existence of these activities in order to litigate their lawfulness. To obtain relief of any kind in this case, Plaintiffs must present evidence of "specific facts" showing that they "are among the [persons] injured" by the Government's alleged unlawful conduct. *Amnesty Int'l*, 133 S. Ct. at 1149; *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 563 (1992) (internal quotation marks and citations omitted). In other words, they must point to specific facts demonstrating that the NSA has collected the contents of, and metadata pertaining to, their communications.

This is the very information—whether or not particular individuals have been the targets of, or subject to, collection under the challenged NSA intelligence programs—that the DNI has concluded would pose a risk of exceptionally grave damage to national security if disclosed. Public DNI Decl. ¶¶ 10-11, 17-19. Plaintiffs assert that establishing whether they have been subjected to "bulk, untargeted surveillance" would "not require any inquiry into or disclosure of the identities of those whom the government is targeting for surveillance." Pls.' Resp. at 18. But that response, as discussed above, reflects a profound misunderstanding of (or unwillingness to acknowledge) the question at hand. *See Halkin v. Helms*, 598 F.2d 1, 8 (D.C. Cir. 1978) (rejecting argument "that admission or denial of the fact of acquisition of [plaintiffs'] communications … would not reveal which circuits NSA has targeted" as "naïve"). Revealing whether or not particular individuals have been subject to collection—even if they themselves are not *targets* of collection—nevertheless could alert adversaries, including foreign terrorist organizations, to information confirming whether their own communications have been subject

to surveillance, or whether their channels of communications have been or remain secure. *See id.*; Public DNI Decl. ¶ 34; Public NSA Decl. ¶ 35-37.[11]

The potentially grave damage to national security of such disclosures is not reduced by the fact that the Government has now declassified the existence of the NSA intelligence programs whose legality Plaintiffs seek to contest. The courts, including the Ninth Circuit, have long appreciated that official confirmation of general information about an intelligence program (such as its existence), does not eliminate the risk to national security of compelling further disclosures of information about the program's details. *Jeppesen*, 614 F.3d at 1086, 1090 (official acknowledgment of existence of CIA extraordinary rendition program did not preclude details of program remaining state secrets if details' disclosure would risk harm to national security); *Al-Haramain*, 507 F.3d at 1203 (concluding that even though the Government had publicly acknowledged the existence of the Terrorist Surveillance Program, disclosing whether the plaintiff had been surveilled would compromise national security).[12]

[11] To the extent Plaintiffs base their argument on the premise that they are challenging programs of "mass, untargeted surveillance" of all Americans' communications, Pls.' Resp. at 16, they are confusing allegation with fact. As we have explained before during the course of this litigation, Plaintiffs' allegations that the NSA has indiscriminately collected the contents of millions of U.S. persons' communications since the September 11, 2001, terrorist attacks are false. Public DNI Decl. ¶ 36. Plaintiffs' naked assertion (Pls.' Resp. at 15) that the Government has acknowledged collecting "everyone's" communications records under the NSA's telephony and Internet metadata programs is also false. While the Government has acknowledged that the NSA's metadata programs have involved bulk collection, they have never captured information on all (or virtually all) telephone calls or Internet-based communications made and/or received in the U.S. *See In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted]*, 2013 WL 5741573, at *1 n.5 (F.I.S.C. Aug. 29, 2013). Therefore, to prove their standing to challenge each of these respective programs, Plaintiffs will require evidence regarding the scope of collection under each of these programs, the disclosure of which, in the judgment of the DNI, could be expected to cause exceptionally grave harm to national security. Public DNI Decl. ¶¶ 39-41; Public NSA Decl. ¶¶ 21-27, 42-47.

[12] *See also ACLU v. U.S. Dep't of Defense*, 628 F.3d 612, 620-22 (D.C. Cir. 2011) (Government's decision to disclose some information about CIA interrogation program did not prevent withholding of information regarding the use of specific techniques on specific detainees); *Wilner v. NSA*, 592 F.3d 60, 69 (2d Cir. 2009) (Government's decision to make public the existence of the Terrorist Surveillance Program did not require disclosure of specific methods used, targets of surveillance, or information obtained); *El-Masri*, 479 F.3d at 308-11 (4th Cir. 2007) (even assuming that existence of CIA rendition program no longer remained a state secret, details of program's means and methods remained privileged); *Halkin v. Helms*, 690 F.2d 979, 993-94 (D.C. Cir. 1982) ("*Halkin II*") (disclosure of CIA station's existence did not require disclosure of activities carried on there); *Salisbury v. United States*, 690 F.2d 966, 971 (D.C. Cir. 1982) (admission that Government had previously monitored communications between U.S. and Hanoi did not require disclosure of whether plaintiff's communications had been intercepted); *Terkel v. AT&T*, 441 F. Supp. 2d 899, 912, 918-19 (N.D. Ill. 2006).

The DNI has determined that it would pose a threat of grave damage to national security to disclose information about targets and subjects of collection under the challenged NSA intelligence programs, notwithstanding the disclosures that have been made regarding the programs since June 2013. Public DNI Decl. ¶¶ 5-11. The basis for that conclusion is well documented in both the public and classified, *ex parte* declarations submitted by the DNI and the NSA in support of his renewed assertion of privilege, and the DNI's judgment that disclosure of that information would still be harmful to national security is entitled to "utmost deference" by the courts. *Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998).[13] Thus, contrary to Plaintiffs' assertion that it remains the Government's burden to "demonstrate[e] that litigating [their] claims will harm national security," Pls.' Resp. at 18, the Government has already carried that burden. In the face of the Government's showing, it is now Plaintiffs' burden to demonstrate that disclosure of the additional information about the challenged activities required to litigate their standing could not reasonably be expected to result in further harm to national security. They have not done so.

Principally, Plaintiffs contend that because evidence of AT&T's "participat[ion]…in the surveillance" is "already in the public domain, using it to litigate plaintiffs' claims cannot cause any harm." Pls.' Resp. at 18-19. But Plaintiffs point to no competent evidence to support their claims. For example, the Klein and Marcus declarations submitted by Plaintiffs, *see id.* at 18, are premised on hearsay, *e.g.*, Klein Decl. ¶¶ 8, 10, 16, and speculation about the activities conducted in a "secure room" to which Mr. Klein had no access. *See id.* ¶ 17. At best, these declarations make inferences about the *capabilities* of equipment located there almost ten years ago (*see* Klein Decl. ¶ 6; Marcus Decl. ¶¶ 38-48), without any first-hand knowledge or information about the activities actually conducted there, then or now.

[13] *See also CIA v. Sims*, 471 U.S. 159, 180 (1985) ("[I]t is the responsibility of the [intelligence community], 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."); *Jeppesen*, 614 F.3d at 1081-82 ("[i]n evaluating the need for secrecy, 'we acknowledge the need to defer to the Executive…in this area'") (quoting *Al-Haramain*, 507 F.3d at 1203); *El-Masri*, 479 F.3d at 304-05; *Ctr. for Nat'l Security Studies v. U.S. Dep't of Justice*, 331 F.3d 918, 928 (D.C. Cir. 2003) ("we have consistently deferred to executive affidavits predicting harm to the national security"); *Black v. United States*, 62 F.3d 1115, 1119 (8th Cir. 1995).

Similarly, Plaintiffs maintain further that AT&T's participation in NSA intelligence-gathering activities has been "confirmed" by reporting in *The Wall Street Journal* and other media outlets. Pls.' Resp. at 19. But that is a contradiction in terms. Media reports are hearsay and as such they are inadmissible to prove the truth of any matters stated therein, much less of allegations concerning classified Government intelligence programs. *E.g., Stewart v. Wachowski*, 574 F. Supp. 2d 1074, 1090 (C.D. Cal. 2005); *see also Jeppesen*, 614 F.3d at 1087 n.11 (noting "hearsay problems" the plaintiffs would have to overcome to prove their claims without relying on privileged state secrets).[14] Plaintiffs thus lack any competent evidence with which to establish that AT&T (or any other company) participated in the NSA intelligence programs at issue here, let alone when, how, under what authority, and whether they involved the collection of Plaintiffs' own communications or records thereof. Unquestionably, the kind of probing discovery needed (and which Plaintiffs anticipate conducting) to establish whether their providers assisted with NSA intelligence activities, even if attempted via *ex parte* proceedings under § 1806(f), would necessarily risk or require the disclosure of still properly protected national security information.

Plaintiffs also cite then-Chief Judge Walker's decision *Hepting v. AT&T Corp.*, 439 F. Supp. 2d 974 (N.D. Cal. 2006), as support for their argument that no harm to national security would ensue from official confirmation of whether AT&T has assisted in NSA intelligence

[14] Plaintiffs also rely on inferences they draw based on information contained in what they represent to be a "Working Draft" of a classified NSA Office of Inspector General report published on the website of *The Guardian*. Pls.' Resp. at 19 n.8; *see* Declaration of Richard R. Wiebe in Opposition to the Government Defendants' Stay Request (ECF No. 147), ¶ 5. Plaintiffs remark that "[t]he government has never contested the authenticity" of this and other so-called "Snowden documents." Pls.' Resp. at 17. But the Government is not required to confirm or deny the authenticity of purportedly classified documents that third parties claim to have obtained as the result of unauthorized disclosures. Plaintiffs' contention, that because the Government has charged Edward Snowden with unlawful disclosure of classified national security information that it has "vouched for [the] authenticity," Pls.' Resp. at 17, of every document downloaded from a website claiming it to be a "Snowden document," is meritless. *See ACLU v. U.S. Dep't of State*, 878 F. Supp. 2d 215, 224 (D.D.C. 2012) ("generalized and sweeping comments" by Executive Branch officials regarding disclosure of classified documents by WikiLeaks did not constitute acknowledgement that the specific documents at issue were among those published by WikiLeaks); *see also Assassination Archives & Research Ctr. v. CIA*, 334 F.3d 55, 60 (D.C. Cir. 2003) (statements by public officials do not constitute official acknowledgement of the contents of classified documents unless they "precisely track the records sought to be released"); *cf. Schwarz v. Lassen County ex rel. Lassen County Jail*, 2013 WL 5425102, at *10 (E.D. Cal. Sept. 27, 2013) (observing that "any evidence procured off the Internet is adequate for almost nothing" without proper authentication).

activities. Pls.' Resp. at 15. The Government Defendants respectfully submit that the manner in which the Court proceeded in that case—relying on speculation based on limited public information about classified matters implicating national security—was not appropriate and was contrary to law. While Judge Walker stated in *Hepting* that "AT&T and the government have for all practical purposes already disclosed that AT&T assists the government in monitoring communication content," 439 F. Supp. 2d at 991-92, the Government had not then (and never has) officially acknowledged whether AT&T has been a participant in any NSA intelligence activity. *See* Public DNI Decl. ¶¶ 19D, 42-44; Public NSA Decl. ¶ 48. The Court in *Hepting* instead relied on the Government's disclosure "of the general contours" of the Terrorist Surveillance Program ("TSP"), and public statements by AT&T that it "assists the Government in classified matters when asked." *Hepting*, 439 F. Supp. 2d at 992-93.[15] But neither disclosure reveals whether AT&T assisted in any particular activity, or when, how, or under what authority, and the Ninth Circuit's subsequent decision in *Al-Haramain* forecloses the sort of inference and speculation engaged in by the Court in *Hepting* where matters of national security are concerned. In *Al-Haramain* the plaintiff claimed that disclosing whether it had been a target of surveillance under the TSP posed no risk to national security because the "very existence of the TSP, and [the plaintiff's] status as a 'Specially Designated Global Terrorist,' suggest[ed] that the government [was] in fact intercepting [its] communications." 507 F.3d at 1203. The Court of Appeals rejected this reasoning, holding that "judicial intuition about this proposition [was] no substitute for documented risks and threats posed by the potential disclosure of national security information." *Id.* The similar argument advanced by Plaintiffs here regarding AT&T's (or any other company's) alleged participation in NSA intelligence programs must also be rejected.[16]

Plaintiffs also contend that no harm to national security can come from litigation of their standing because "[n]ews organizations of great integrity and well-established track records of

[15] The Court did not, however, rely on Plaintiffs' Klein declaration, or media reports about alleged NSA intelligence activities. *Hepting*, 439 F. Supp. 2d at 990-91.

[16] The Government appealed the *Hepting* decision, but it was remanded and thereafter resolved on the basis of the FISA Amendments Act of 2008, which granted immunity to telecommunications providers sued for allegedly assisting the NSA. *See In re NSA Telecomm. Recs. Lit.*, 671 F.3d 881 (9th Cir. 2011); *Hepting v. AT&T Corp.*, 539 F.3d 1157 (9th Cir. 2008).

accuracy in intelligence reporting … have made repeated reports … disclosing numerous aspects" of those programs. Pls.' Resp. at 20. This line of argument runs into a battery of contrary precedent. Litigants seeking to establish that national security information already resides "in the public domain," Pls.' Resp. at 19, bear the burden of demonstrating that the specific information at issue has been "officially acknowledged," *Wolf v. CIA*, 473 F.3d 370, 378 (D.C. Cir. 2007), through "an intentional, public disclosure made by or at the request of a government officer acting in an authorized capacity by the agency in control of the information at issue." *Pickard v. U.S. Dep't of Justice*, 653 F.3d 782, 787 (9th Cir. 2011). This is a "strict test," *Wilson v. CIA*, 586 F.3d 171, 186 (2d Cir. 2009), that distinguishes between official and documented disclosures, which can place national security information in the public domain, and unauthorized disclosures such as leaks by current and former agency employees (or contractors), private-party allegations purporting to reveal the conduct of intelligence agencies, anonymously sourced press reports, and most relevant here, widespread media and public speculation, which courts do not regard as placing classified national security information in the public domain.[17]

Courts distinguish so firmly between official and unofficial disclosures because of the "critical difference" between them. *Id.* (quoting *Fitzgibbon v. CIA*, 911 F.2d 755, 765 (D.C. Cir. 1990)); *Alsawam v. Obama*, 764 F. Supp. 2d 11, 15 (D.D.C. 2011). As various courts of appeals have observed, "'[i]t is one thing for a reporter …to speculate or guess that a thing may be so or even, quoting undisclosed sources, to say that it is so; it is quite another for one in a position to know of it officially to say that it is so.'" *ACLU v. U.S. Dep't of Defense*, 628 F.3d at 621-22 (quoting *Alfred A. Knopf, Inc. v. Colby*, 509 F.2d 1362, 1370 (4th Cir. 1965)); *see Stein v. Dep't of Justice*, 662 F.2d 1245, 1259 (7th Cir. 1981). Official acknowledgment by an authoritative source may remove "lingering" and "unresolved doubt[s] . . . in the minds . . . of potential or

[17] *See Ameziane v. Obama*, 699 F.3d 488, 498 (D.C. Cir. 2010) (re-issued Oct. 5, 2012); *EPIC v. NSA*, 678 F.3d 926, 933 n.5 (D.C. Cir. 2012) (public speculation regarding a collaborative relationship between the NSA and Google); *ACLU v. U.S. Dep't of Defense*, 628 F.3d at 621-22 (rejecting argument that information withheld by the CIA was so widely disseminated that its disclosure could not cause harm to national security); *Wilson*, 586 F.3d at 186-87; *Judicial Watch v. U.S. Dep't of Justice*, 898 F. Supp. 2d 93, 107-08 (D.D.C. 2012); *ACLU v. U.S. Dep't of Defense*, 752 F. Supp. 2d 361, 367-68 (S.D.N.Y. 2010), citing *Afshar v. Dep't of State*, 702 F.2d 1125, 1130 (D.C. Cir. 1983); *Cozen O'Connor v. U.S. Dep't of the Treasury*, 570 F. Supp. 2d 749, 788 (E.D. Pa. 2008); *El-Masri v. Tenet*, 437 F. Supp. 2d 530, 538 (E.D. Va. 2006); *Edmonds v. U.S. Dep't of Justice,* 323 F. Supp. 2d 65, 77 (D.D.C. 2004).

actual adversaries" regarding the truth of information reported (or speculation advanced) in the public domain. *Frugone v. CIA*,169 F.3d 772, 774 (D.C. Cir. 1999); *see Wilson*, 586 F.3d at 195 ("anything short of [an official] disclosure necessarily preserves some increment of doubt regarding the reliability of the publicly available information"); *Military Audit Project v. Casey*, 656 F.2d 724, 744 (D.C. Cir. 1981). As a result, official acknowledgment "might well be new information that could cause damage to the national security," *Afshar*, 702 F.2d at 1130; *see Abbotts Nuclear Regulatory Comm'n*, 766 F.2d 604, 607-08 (D.C. Cir. 1985), by "lead [ing] [our adversaries] to take some action that otherwise would not be taken." *Stein*, 662 F.2d at 1259. *See also Public Citizen v. Dep't of State*, 11 F.3d 198, 201 (D.C. Cir. 1993); *Bareford v. Gen. Dynamics Corp.*, 973 F.2d 1138, 1144 (5th Cir. 1992).[18]

Hence, it is well-established in the case law, contrary to Plaintiffs' arguments, that "the fact that information exists in some form in the public domain does not necessarily mean that official disclosure will not cause harm" to national security. *Wolf*, 473 F.3d at 378. Here, the DNI has attested to his judgment that confirmation or denial of the very facts that Plaintiffs must prove in order to establish their standing would pose a risk of exceptionally grave damage to national security, notwithstanding the disclosures regarding NSA intelligence programs that have

[18] Courts have also long recognized that disclosures of information differing in their specificity or particulars from that which already has been officially acknowledged can provide "additional information" to our adversaries "that would be harmful to national security." *Edmonds*, 323 F. Supp. 2d at 77; *see also El-Masri*, 479 F.3d at 308-09; *Fitzgibbon*, 911 F.2d at 766. It is therefore firmly established that the Government, having concluded in one case that a disclosure of intelligence information is permissible, or even advisable, in the national interest, is not "estopped" from concluding in the next case that a similar disclosure "may lead to an unacceptable risk" of harm to national security. *Sims*, 471 U.S. at 180-81; *Public Citizen*, 11 F.3d at 201; *Halkin II*, 690 F.2d at 994; *Salisbury*, 690 F.2d at 971; *Stein*, 662 F.2d at 1258-59. Accordingly, Plaintiffs err when they argue that the Government's decision to permit "telecommunications providers like AT&T to reveal that they are subject to FISA surveillance orders" is "inconsistent" with the Government's assertion of the state secrets privilege over the identity of providers participating in the alleged NSA intelligence programs. *See* Pls.' Br. at 20 (citing ECF No. 178, at Ex. E). Under the Government's decision to allow providers to report aggregate numbers of FISA content orders and "customer selectors targeted," the identities of the persons targeted for surveillance under those orders remain classified. Moreover, the Government's decision does not apply to the identities of providers that have participated in particular NSA intelligence programs, including the bulk collection of telephony and Internet metadata. ECF No. 178, Ex. E at 2 n.1. Thus, the information providers are now permitted to disclose about aggregate numbers of orders and selectors does not include what Plaintiffs need to prove here: that the contents of and metadata pertaining to their communications have been collected by the NSA with the assistance of their carriers. Whether that is so or not is still properly held, therefore, as a privileged state secret.

occurred since June 2013. As discussed above, any effort to establish whether Plaintiffs have standing to maintain this action, whether through proceedings under § 1806(f) or otherwise, would inherently risk or require disclosure of facts over which Director Clapper has asserted privilege, thus inviting risks to national security that this Court is obligated to avoid. *Amnesty Int'l*, 133 S. Ct. at 1149 n.4.

CONCLUSION

For the reasons explained above, and in our initial response to the Court's four threshold questions: (1) the Government does not dispute that the Court's ruling on FISA preemption would apply equally to Plaintiffs' constitutional claims as it does to their statutory claims; (2) nevertheless, the procedural mechanism for *ex parte, in camera* review under § 1806(f) applies only to the extent that Plaintiffs can show, without reliance on privileged state secrets, that they are "aggrieved persons" whose communications have been subject to "electronic surveillance" within the meaning of FISA; (3) Plaintiffs cannot litigate their standing, even through *ex parte* proceedings under § 1806(f), without risking or requiring disclosures of privileged state secrets that could reasonably be expected to cause exceptionally grave harm to national security, and (4) that remains so notwithstanding the disclosures and declassification decisions regarding NSA intelligence activities that have occurred since June 2013.

Dated: March 7, 2014

Respectfully submitted,

STUART F. DELERY
Assistant Attorney General

JOSEPH H. HUNT
Director, Federal Programs Branch

ANTHONY J. COPPOLINO
Deputy Branch Director

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

MARCIA BERMAN
Senior Trial Counsel
marcia.berman@usdoj.gov

BRYAN DEARINGER
Trial Attorney

RODNEY PATTON
Trial Attorney

U.S. Department of Justice, Civil Division
20 Massachusetts Avenue, NW, Rm. 6102
Washington, D.C. 20001
Phone: (202) 514-3358
Fax: (202) 616-8470

Attorneys for the Government Defendants