CASE NO. 10-15616
(consolidated for calendaring purposes with No. 10-15638)

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

CAROLYN JEWEL, TASH HEPTING, GREGORY HICKS, ERIC KNUTZEN, AND JOICE WALTON,

PLAINTIFFS-APPELLANTS,

V.

NATIONAL SECURITY AGENCY, *ET AL.*,

DEFENDANTS-APPELLEES.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE
NORTHERN DISTRICT OF CALIFORNIA, NO. 08-CV-04373-VRW
THE HONORABLE VAUGHN R. WALKER, CHIEF UNITED STATES DISTRICT JUDGE, PRESIDING

APPELLANTS' REPLY BRIEF

RACHAEL E. MENY
PAULA L. BLIZZARD
MICHAEL S. KWUN
AUDREY WALTON-HADLOCK
KEKER & VAN NEST LLP
710 Sansome Street
San Francisco, CA 94111
Telephone: (415) 391-5400
Facsimile: (415) 397-7188

THOMAS E. MOORE III
THE MOORE LAW GROUP
228 Hamilton Ave., 3d Fl.
Palo Alto, CA 94301
Telephone: (650) 798-5352
Facsimile: (650) 798-5001

ARAM ANTARAMIAN
LAW OFFICE OF ARAM ANTARAMIAN
1714 Blake Street
Berkeley, CA 94703
Telephone: (510) 841-2369

RICHARD R. WIEBE
LAW OFFICE OF RICHARD R. WIEBE
One California Street, Suite 900
San Francisco, CA 94111
Telephone: (415) 433-3200
Facsimile: (415) 433-6382

CINDY A. COHN
LEE TIEN
KURT OPSAHL
KEVIN S. BANKSTON
JAMES S. TYRE
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Legislative Materials

INTRODUCTION

As plaintiffs' opening brief explains, the district court erred in dismissing, *sua sponte*, this action on the ground that plaintiffs had failed to plead any injury satisfying Article III's standing requirements. Each plaintiff has had his or her individual communications and communications records intercepted and acquired by the defendants. That is a concrete and particularized injury to each plaintiff and is more than sufficient to satisfy Article III.

The government defendants[1] make no serious effort to defend the district court's error. Instead, they proffer their own, equally erroneous, alternative grounds for dismissal. They invent a wholly novel transmutation of the state secrets privilege into a prudential standing doctrine. There is no basis in prudential standing law for doing so, and no necessity to further expand the state secrets privilege in this manner to further hobble injured plaintiffs from obtaining redress for violations of their civil liberties.

---

[1] Only the government defendants—i.e., the United States, the agency defendants and the official-capacity defendants—defend the district court's dismissal on appeal. The individual-capacity defendants have not filed a brief and have waived making any defense of the judgment. The government defendants purport to argue on behalf of the individual-capacity defendants, Govt. Defs. Br. at 24 n.7, but they lack standing or authority to do so. Nor are they correct in suggesting that the individual-capacity defendants were simply executing a lawfully authorized policy created by others. *Id*. The individual-capacity defendants were not low-level functionaries but the principal actors in a plan to violate FISA, other statutes, and the Constitution. *See* AER 16-20, 32, 82-119.

The government defendants also assert, as an alternative ground for affirmance, that plaintiffs will be unable to prove their case without the use of evidence from the government that is protected by the state secrets privilege. This argument fails for three reasons: First, in lawsuits like this one challenging unlawful electronic surveillance, Congress has displaced the state secrets privilege with section 1806(f) of title 50 U.S.C. Section 1806(f) directs courts to use national security evidence, *ex parte* and *in camera*, to determine whether the surveillance was lawfully authorized and conducted. Second, even if the state secrets privilege did apply to this lawsuit, it is impossible to determine at the pleading stage, before there has been any discovery of nonprivileged evidence and before plaintiffs have had the opportunity to present the nonprivileged evidence they already possess, whether plaintiffs will be able to prove their claims with nonprivileged evidence. Third, the assertion of the state secrets privilege by Director of National Intelligence Blair is overbroad and inadequately supported in crucial respects.

ARGUMENT

I. The Government Defendants' Standing Arguments Are Meritless

A. Plaintiffs' Standing Is Straightforward

As plaintiffs demonstrated in their opening brief, they have more than adequately alleged "concrete and particularized" injuries to themselves that satisfy their Article III standing burden at the pleading stage. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992); Appellants' Opening Brief ("AOB") at 4-7, 13-16.

Plaintiffs allege for their injuries that the defendants have intercepted and acquired plaintiffs' own communications—*their* phone calls, emails, instant messages, text messages, and other communications—and records of those communications. Appellants' Excerpts of Record ("ER") 23-25, 29-35, 38-42, 44, 46-47, 49-50, 52-53, 55-56, 58-61, 63, 65, 67, 69-73 (Complaint ¶¶ 7-10, 12-13, 20-24, 50-97, 110-111, 120-21, 129-30, 138, 148-53, 161-64, 173-78, 189-94, 203-08, 214-15, 223-24, 230-31, 237-38, 246-47, 253-54, 260, 264).

These are concrete injuries—defendants have breached the physical, legal, and contractual barriers shielding the privacy of each plaintiff's information and have seized possession of it. These injuries are particular to each plaintiff—the harm plaintiff Jewel suffers when defendants acquire one of her emails is not suffered by anyone else but her. *Lujan*, 504 U.S. at 560 n.1 ("particularized" means "affect[ing] the plaintiff in a personal and individual way"). Accordingly, defendants' interception and acquisition of

each plaintiff's own communications and communications records is a concrete injury particular to that individual plaintiff that satisfies the injury-in-fact requirement for plaintiffs' constitutional and statutory claims. "When the suit is one challenging the legality of government action . . . [and] the plaintiff is himself an object of the action . . . . there is ordinarily little question that the action . . . has caused him injury . . . ." *Lujan*, 504 U.S. at 561-62; *see also* AOB at 28-31.

Plaintiffs additionally have standing for their express statutory causes of action (Counts V-XVI) because of the rule that alleging the invasion of statutory rights satisfies the injury-in-fact requirement. "The actual or threatened injury required by Art. III may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing." *Warth v. Seldin*, 422 U.S. 490, 500 (1975) (internal quotation marks and ellipsis omitted); *see also Massachusetts v. EPA*, 549 U.S. 497, 516 (2007) (" 'Congress has the power to define injuries and articulate chains of causation that will give rise to a case or controversy where none existed before.' "); *Fulfillment Services v. UPS*, 528 F.3d 614, 618-19 (9th Cir. 2008) (same). Importantly, violations of these statutes are complete upon defendants' interception of plaintiffs' communications or communications records, and do not require proof of what subsequent use, if any, defendants made of the communications or records or what the content of those communications and records were.

The government defendants make a cursory argument that plaintiffs have failed to adequately allege injury in fact. Govt. Defs. Br. at 23. They repeatedly contend that the complaint's allegations are "bare speculation" with "no support." *Id*. But these conclusory pejoratives are not supported by any actual analysis: the government defendants avoid addressing even a single specific fact alleged in plaintiffs' complaint. Their evasion is understandable, given the complaint's specific and concrete allegations, with numerous supporting facts, that each plaintiff's own communications and communications records were intercepted and acquired by defendants. *See* AOB at 4-7, 14-16.

The government defendants further err in contending that to avoid a *sua sponte* dismissal at the pleading stage plaintiffs must support their allegations with evidence. At the pleading stage, allegations alone are sufficient to establish standing, and they may be general allegations. *Bennett v. Spear*, 520 U.S. 154, 168 (1997) (" '[a]t the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice, for on a motion to dismiss we "presume that general allegations embrace those specific facts that are necessary" ' "); *Oregon v. Legal Services Corp.*, 552 F.3d 965, 969 (9th Cir. 2009) (same).

Bennett demonstrates how general allegations can create a presumption of specific harm. The plaintiffs were farmers who used irrigation water from a reservoir; they challenged the validity of a report concluding that two fish species were endangered. For their injury, they

alleged that the report would lead to a reduction in the total amount of water available for irrigation from the reservoir, but did not allege that this would cause any reduction in their individual water allocations. Notwithstanding the absence of any allegation of a specific harm to the plaintiffs from this government action of widespread consequence, the Supreme Court found it "easy to presume specific facts under which petitioners will be injured." *Bennett*, 520 U.S. at 168. Here, the Court need not take the additional step of presuming harm, because each plaintiff has expressly pleaded interception and acquisition of his or her own communications.

Moreover, although they need not do so at the pleading stage, plaintiffs have proffered evidence in support of their allegations substantial enough to demonstrate a *prima facie* case of injury in fact. Appellants' Additional Excerpts of Record ("AER") 8-66; Appellants' Request for Judicial Notice ("RJN"), Exs. A, B; *see Warth*, 422 U.S. at 501 (when standing is challenged, court may allow "plaintiff to supply, by amendment to the complaint or by affidavits, further particularized allegations of fact deemed supportive of plaintiff's standing"). This evidence and its import is described further in section III(B) below.[2]

[2] The government defendants do not dispute that it was error to dismiss plaintiffs' complaint without leave to amend. AOB 40-41.

B. The State Secrets Privilege Is Not A Prudential Standing Doctrine

The government defendants make the unprecedented suggestion that the state secrets privilege should be transformed into a novel prudential standing barrier. Govt. Defs. Br. at 19-23. Their attempt is remarkable for its lack of supporting authority, its failure to address contrary controlling authority, and its disregard of the facts alleged in plaintiffs' complaint.

Plaintiffs' express statutory causes of action are not subject to the prudential standing doctrine. When Congress enacts a statutory cause of action, it negates prudential standing barriers. "Congress may grant an express right of action to persons who otherwise would be barred by prudential standing rules." *Warth*, 422 U.S. at 501. Because "Congress, intending to protect [persons such as plaintiffs] . . . from suffering the kind of injury here at issue, intended to authorize this kind of suit . . ., [plaintiffs] satisfy 'prudential' standing requirements," including the government defendants' proposed state-secrets prudential standing bar. *Federal Election Commission v. Akins*, 524 U.S. 11, 20 (1998). And because Congress has directed that plaintiffs' statutory claims go forward, it would be nonsensical to invent a novel state-secrets-based prudential standing doctrine that would simultaneously prohibit plaintiffs' constitutional claims based on the same facts and the same evidence from going forward.

The rule forbidding using prudential standing rules to thwart an express statutory cause of action was explained at length in plaintiffs'

opening brief. AOB 22-28, 38-40. Having no answer, the government defendants simply refuse to address this controlling principle of law or any of the authority supporting it. They ignore, moreover, that the "specific judicial procedures [Congress] has established under FISA to regulate foreign intelligence surveillance," Govt. Defs. Br. at 13-14, include plaintiffs' causes of action under section 1810 of title 50 U.S.C. ("section 1810"). They equally ignore that in section 1806(f) of title 50 U.S.C. ("section 1806(f)"), discussed in section II below, "Congress . . . ensure[d] that appropriate measures are in place to prevent disclosure of information concerning intelligences activities," Govt. Defs. Br. at 14, while permitting litigation of unlawful surveillance claims to go forward on the merits.

In addition to being foreclosed by the prudential standing doctrine, the government defendants' position is contrary to the state secrets doctrine itself. "[T]he state secrets privilege is an evidentiary privilege rooted in federal common law," not a standing doctrine, and ordinarily its effect is simply that "[t]he plaintiff's case then goes forward based on evidence not covered by the privilege." *Kasza v. Browner*, 133 F.3d 1159, 1167, 1166 (9th Cir. 1998). This Court's recent en banc opinion in *Mohamed v. Jeppesen*, discussed in more detail in section III below, makes clear that the two "rare circumstances" in which the state secrets privilege permits threshold dismissal of a lawsuit have nothing to do with the prudential standing doctrine. *Mohamed v. Jeppesen*, 614 F.3d 1070, 1084, 1087, 1089

(9th Cir. 2010) (en banc). Nor has any other state secrets privilege decision ever held that the state secrets doctrine is a prudential standing doctrine.

Lacking any supporting authority and unwilling to address controlling contrary authority, the government defendants instead rest their argument on one erroneous assertion after another. They err in asserting that it is "plaintiffs' claims" that "seek to prohibit specific intelligence methods allegedly used by NSA." Govt. Defs. Br. at 19. Those methods—untargeted, suspicionless dragnet surveillance—are *already* prohibited both by Congress in statute after statute and by the Founders in the Constitution, and Congress has directed the courts to enforce those prohibitions in private civil actions brought by those like plaintiffs who have been unlawfully surveilled.

Nor is it true that "Congress notably has not authorized the federal district courts to undertake the kind of review of alleged intelligence activities . . . that plaintiffs seek in these cases." Govt. Defs. Br. at 23. Congress has expressly authorized the courts to adjudicate plaintiffs' claims, most notably by creating in section 1810 civil liability in district court for FISA violations and by requiring in section 1806(f) that district courts "determine whether the surveillance of the aggrieved person was lawfully authorized and conducted," notwithstanding the presence of state secrets. *See* section II, below. Nor did Congress' 2008 enactment of the FISA Amendments Act (Govt. Defs. Br. at 22) change anything on this score—to the contrary, those amendments intentionally left untouched lawsuits against

government agencies or officials. 50 U.S.C. § 1885(5); *accord*, S. Rep. No. 110-209 at 8 (2007) ("The Committee does not intend for this section to apply to, or in any way affect, pending or future suits against the Government as to the legality of the President's program.").

Finally, it is fatally incomplete to say that "The Constitution gives the President authority and responsibility to protect the security of the United States." Govt. Defs. Br. at 19. The national security powers are "powers granted *jointly* to the President and Congress." *Hamdan v. Rumsfeld*, 548 U.S. 557, 591 (2006) (emphasis added). Congress has exercised its national security powers to grant plaintiffs standing to pursue their claims alleging unlawful surveillance, and the courts have no warrant to defy Congress by refusing to adjudicate those claims.

C. The Government Defendants' Prudential Generalized-Grievance Argument Is Meritless

The government defendants make only a prudential "generalized grievance" argument, not one based on Article III. Govt. Defs. Br. at 18. This argument lacks merit. As previously explained, where an Article III injury in fact exists and where Congress has created an express statutory cause of action, there are no prudential standing barriers. *Akins*, 524 U.S. at 20; *Warth*, 422 U.S. at 501.

Plaintiffs' injuries are not a generalized grievance under any definition. The capture of plaintiff Hepting's own telecommunications is an injury particular to him and is not even shared by plaintiff Walton, much less

by the world at large. That others may also have suffered parallel, but distinct and separate, injuries does nothing to diminish the particularity or the concreteness of the injury to plaintiff Hepting: " '[I]t does not matter how many persons have been injured by the challenged action' " so long as "the party bringing suit . . . show[s] that the action injures him in a concrete and personal way.' " *Massachusetts v. EPA*, 549 U.S. at 517. "Once it is determined that a particular plaintiff is harmed by the defendant, and that the harm will likely be redressed by a favorable decision, that plaintiff has standing—regardless of whether there are others who would also have standing to sue." *Clinton v. City of New York*, 524 U.S. 417, 434-36 (1998); *accord, Akins*, 524 U.S. at 24 ("where a harm is concrete, though widely shared, the Court has found 'injury in fact' "); *Newdow v. Lefevre*, 598 F.3d 638, 642 (9th Cir. 2010) (same).

To the extent that the government defendants argue that plaintiffs' claims raise issues that should be acted upon by the political branches (Govt. Defs. Br. at 18-19), the answer is that the political branches have already acted and have directed the courts to adjudicate plaintiffs' claims. Congress has enacted, and Presidents have signed, the statutes under which plaintiffs sue, imposing limits on the Executive's power to conduct electronic surveillance and creating express causes of action to enforce those limitations.

II. Section 1806(f) Displaces The State Secrets Privilege Here

The government defendants argue that the dismissal of plaintiffs' action should be affirmed on the alternative ground that the state secrets privilege applies to evidence in this case and deprives plaintiffs of evidence essential to proving their *prima facie* case. This argument fails because Congress has displaced the state secrets privilege here by the statutory directive of section 1806(f).

A. Congress Has Displaced The State Secrets Privilege In Cases Involving Electronic Surveillance

Congress recognized that in civil actions challenging the lawfulness of electronic surveillance the evidence will often include sensitive national security information that should not be publicly disclosed. In section 1806(f), Congress established a procedure enabling those actions to go forward to a decision on the merits of the legality of the surveillance while protecting the secrecy of the information on which the decision is based. Rather than excluding national security evidence, as would occur under the state secrets privilege, Congress instead displaced the state secrets privilege and directed courts to use all of the relevant national security evidence, reviewed *in camera* and *ex parte*, as the basis for deciding the legality of the surveillance.[3]

[3] In the district court below, plaintiffs raised section 1806(f)'s displacement of the state secrets privilege in opposition to the government's assertion of the state secrets privilege. Dkt. # 29 at 14-18.

In relevant part, section 1806(f) provides:

> . . . whenever *any motion or request* is made by an aggrieved person pursuant to any other statute or rule of the United States or any State . . . 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*.

§ 1806(f) (emphasis added).[4]

Congress' purpose in section 1806(f) is what its text states it to be: to provide a method "to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted" in those instances where the government tells the court that "disclosure or an adversary hearing would harm the national security of the United States." § 1806(f).

The overlap between section 1806(f) and the state secrets privilege is self-evident. The state secrets privilege is a common-law doctrine that addresses "exceptional circumstances [in which] courts must act in the interests of the country's national security to prevent disclosure of state secrets." *Mohamed*, 614 F.3d at 1077. The subject matter of section 1806(f) is the same: circumstances in which "disclosure [of evidence] or an adversary hearing would harm the national security of the United States."

[4] The full text of section 1806(f) is set forth in the statutory appendix.

§ 1806(f). Like the state secrets privilege, section 1806(f) is triggered by the government's assertion that disclosure of evidence or litigation proceedings would threaten national security. *Compare United States v. Reynolds*, 345 U.S. 1 (1953) (state secrets privilege requires "a formal claim of privilege," *id*. at 7-8, demonstrating that "there is a reasonable danger that compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged," *id*. at 10) *with* § 1806(f) ("an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States").

In cases involving electronic surveillance, section 1806(f) displaces and supersedes the common-law state secrets privilege. Congress expressly provided that section 1806(f) applies "notwithstanding any other law," thus confirming its intent to displace the state secrets privilege in cases challenging the lawfulness of electronic surveillance.[5] Congress required the courts to decide the merits of the lawfulness of the surveillance using

[5] "Congress, of course, has plenary authority over the promulgation of evidentiary rules for the federal courts." *Usery v. Turner Elkhorn Mining Co.*, 428 U.S. 1, 31 (1976). In enacting Federal Rule of Evidence 501 (Pub. L. No. 93-595, § 1, 88 Stat. 1933), Congress provided that "the privilege of . . . [the] government . . . shall be governed by the principles of the common law" "[e]xcept as otherwise . . . provided by Act of Congress." *See also* H.R. Rep. No. 93-650 (1973), *reprinted in* 1974 U.S.C.C.A.N. 7075, 7082 (explaining that Rule 501 encompasses the "secrets of state" privilege); S. Rep. No. 93-1277 (1974), *reprinted in* 1974 U.S.C.C.A.N. 7047, 7058 (same). Section 1806(f) is an act of Congress that "otherwise . . . provide[s]" for the admission of state secrets evidence, thereby superseding the common-law state secrets privilege.

national security evidence, *in camera* and *ex parte*, rather than applying the state secrets privilege to exclude that evidence. "The statute, unlike the common law state secrets privilege, provides a detailed regime to determine whether surveillance 'was lawfully authorized and conducted.' " *Al-Haramain Islamic Foundation, Inc. v. Bush* ("*Al-Haramain I*"), 507 F.3d 1190, 1205 (9th Cir. 2007). Section 1806(f) requires courts "to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted" by "review[ing] in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary." § 1806(f).

Section 1806(f) leaves no room for the state secrets privilege to operate. In cases to which section 1806(f) applies, it and the state secrets privilege are mutually exclusive. Applying the state secrets privilege in such a case would mean nullifying section 1806(f), contrary to Congress' intent.[6]

[6] In *Al-Haramain I*, this Court remanded the issue of whether section 1806(f) displaces the state secrets privilege. 507 F.3d at 1206. On remand, the district court held that section 1806(f) displaces the state secrets privilege. *Al-Haramain Islamic Foundation, Inc. v. Bush* ("*Al-Haramain II*"), 564 F.Supp.2d 1109, 1124 (N.D. Cal. 2008). Accordingly, the issue, which is a question of law, is now ripe for this Court to decide. Deciding this issue now will greatly expedite the course of proceedings on remand.

B. FISA's Statutory Scheme And Legislative History Confirm That Section 1806(f) Preempts The State Secrets Privilege

1. Congress Enacted FISA To Establish Comprehensive Control Over National Security Electronic Surveillance

FISA's statutory scheme and legislative history further confirm section 1806(f)'s preemption of the state secrets privilege. FISA was enacted in 1978 in the wake of a Senate investigation (known as the "Church Committee") revealing that for many decades the Executive, without any warrants or other lawful authority, had been conducting massive, secret dragnet surveillance invading the privacy and violating the constitutional rights of thousands of ordinary Americans. S. Rep. No. 94-755, *Book II: Intelligence Activities and the Rights of Americans* ("Book II"), (1976).[7]

The Church Committee concluded that the "massive record of intelligence abuses over the years" had "undermined the constitutional rights of citizens . . . primarily because checks and balances designed by the framers of the Constitution to assure accountability have not been applied." Book II at 290, 289. The Committee urged "fundamental reform," recommending legislation to "make clear to the Executive branch that [Congress] will not condone, and does not accept, any theory of inherent or implied authority to violate the Constitution, the proposed new charters, or

[7] Available at http://www.aarclibrary.org/publib/contents/church/contents_church_reports.htm.

any other statutes." *Id*. at 289, 297. Citing *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952), it noted that "there would be no such authority after Congress has . . . covered the field by enactment of a comprehensive legislative charter" that would "provide the exclusive legal authority for domestic security activities" and prohibit "warrantless electronic surveillance." Book II at 297 & n.10.

The Committee recommended the creation of civil remedies for unlawful surveillance. The purpose of these remedies would be both to "afford effective redress to people who are injured by improper federal intelligence activity" and "to deter improper intelligence activity." Book II at 336. The Committee also anticipated section 1806(f)'s displacement of the state secrets privilege to permit civil claims of unlawful surveillance to be litigated, stating that "courts will be able to fashion discovery procedures, including inspections of materials in chambers, and to issue orders as the interests of justice require, to allow plaintiffs with substantial claims to uncover enough factual material to argue their case, while protecting the secrecy of governmental information in which there is a legitimate security interest." *Id*. at 337.

FISA was Congress' response to the Church Committee's revelations and recommendations: "This legislation is in large measure a response to the revelations that warrantless electronic surveillance in the name of national security has been seriously abused." S. Rep. No. 95-604(I) at 7 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3908. FISA implemented the

Church Committee's recommendations by imposing strict limits on the Executive's power to conduct electronic surveillance. *E.g.*, S. Rep. No. 95-604(I) at 8, 1978 U.S.C.C.A.N. at 3910 (FISA "curb[s] the practice by which the Executive Branch may conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it"); S. Rep. No. 94-1035 at 11 (1976) ("the past record establishes clearly that the executive branch cannot be the sole or final arbiter of when such proper circumstances exist"), 20 ("executive self-restraint, in the area of national security electronic surveillance, is neither feasible nor wise"). By providing "effective, reasonable safeguards to ensure accountability and prevent improper surveillance" by the Executive, FISA restored the balance between the protection of civil liberties and the protection of the national security. S. Rep. No. 95-604(I) at 7, 1978 U.S.C.C.A.N. at 3908.

2. Section 1806(f) Is An Essential Element Of Congress' Comprehensive Scheme For Judicially Enforcing The Limitations It Has Imposed On Electronic Surveillance

To ensure that the Executive could not evade the limits Congress imposed on electronic surveillance, Congress expressly provided in FISA that FISA and the domestic law enforcement electronic surveillance provisions of title 18 (originally enacted as Title III of the Omnibus Crime Control and Safe Streets Act of 1968) are the exclusive means by which the Executive may conduct electronic surveillance within the United States:

> [P]rocedures in this chapter [chapter 119 of title 18, the codification of Title III] and the Foreign Intelligence Surveillance Act of 1978 shall be the *exclusive means* by which electronic surveillance, as defined in section 101 of such Act [50 U.S.C. § 1801], and the interception of domestic wire, oral, and electronic communications may be conducted.

Pub. L. No. 95-511; 92 Stat. 1783, 1797 (emphasis added); *codified at* 18 U.S.C. § 2511(2)(f). Congress reiterated this exclusivity recently when it enacted the FISA Amendments Act of 2008. 50 U.S.C. § 1812.

Given the history of past executive abuses, Congress knew that its mandate of statutory exclusivity would become a reality only if it also created mechanisms for judicial enforcement of the comprehensive procedural and substantive limitations on electronic surveillance it had imposed on the Executive. Accordingly, FISA provides for judicial review of national security electronic surveillance *before* it occurs, requiring (with limited exceptions) that the government obtain a warrant from the Foreign Intelligence Surveillance Court ("FISC") before conducting surveillance. *See* 50 U.S.C. § 1804. The warrant requirement allows the FISC to enforce the substantive limitations FISA imposes on surveillance; for example, FISA limits the targeting of American citizens for surveillance by requiring that the FISC first determine, upon a showing of probable cause, that the target is an "agent of a foreign power." *Id.*; 50 U.S.C. § 1801(b).

FISA also authorizes the courts to review the legality of governmental surveillance *after* it has occurred. It does so by creating criminal and civil liability for unlawful electronic surveillance (50 U.S.C. §§ 1809, 1810) and

by providing for the exclusion in criminal cases of unlawfully obtained surveillance evidence (50 U.S.C. § 1806(e)). It also does so by creating section 1806(f)'s requirement that courts use national security evidence to determine the legality of surveillance, instead of excluding that evidence under the state secrets privilege. Both FISA's civil liability provision, section 1810, and section 1806(f)'s mandate for using national security evidence were enacted in 1978 as part of the original FISA statute and have never been amended or cut back. Pub. L. No. 95-511, §§ 106(f), 110; 92 Stat. at 1794, 1796.

FISA's civil remedy provisions and section 1806(f)'s directive thus are both essential elements of FISA's statutory scheme. Section 1806(f) provides the practical means by which the civil liability created to protect the exclusivity of FISA and Title III and enforce substantive limitations on surveillance can be litigated without endangering the national security.[8]

C. Section 1806(f) Encompasses Civil And Criminal Cases In Which The Lawfulness Of Electronic Surveillance Is At Issue

Section 1806(f) applies "whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States

[8] Congress similarly enacted the Classified Information Procedures Act (CIPA), 18 U.S.C. App. 3, to make it possible to litigate criminal cases involving state secrets. CIPA permits courts to use a variety of procedures, including summaries in place of classified evidence, to enable litigation to go forward consistent with due process.

or any State before any court or other authority of the United States or any state to discover or obtain applications or orders or other materials relating to electronic surveillance." This text encompasses civil cases like this one in which the lawfulness of electronic surveillance is at issue.

Section 1806(f)'s application to civil cases is a necessary part of the statutory scheme. Without section 1806(f), the civil enforcement mechanism that Congress created to ensure FISA's exclusivity would be toothless. By asserting the state secrets privilege to block judicial review of the lawfulness of its activities, the Executive could free itself from the restraints of FISA and once again "conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it." S. Rep. No. 95-604(I) at 8, 1978 U.S.C.C.A.N. at 3910.

FISA's legislative history confirms that section 1806(f) applies to civil cases. The Senate and the House of Representatives proposed different versions of the provision that became section 1806(f). H.R. Conf. Rep. No. 95-1720 at 31-32 (1978), *reprinted in* 1978 U.S.C.C.A.N. 4048, 4060-61 ("FISA Conf. Rep."). The House bill had two separate procedures for determining the legality of electronic surveillance, one for criminal cases and one for civil cases; the Senate bill had a single procedure for both criminal and civil cases. *Id.*

In the end, Congress adopted a modified version of the Senate procedure, deeming a single procedure sufficient both for criminal cases in which a defendant is seeking to suppress surveillance evidence and for civil

cases in which a plaintiff is seeking a determination of the legality of electronic surveillance in order to vindicate constitutional and statutory rights:

> The conferees [of the joint House and Senate Committee of Conference] agree that an in camera and ex parte proceeding is appropriate for determining the lawfulness of electronic surveillance *in both criminal and civil cases*.

FISA Conf. Rep. at 32, 1978 U.S.C.C.A.N. at 4061 (emphasis added).

Section 1806(f) applies to all civil claims challenging the lawfulness of electronic surveillance, whether brought under section 1810 of FISA or some other provision (e.g., the Constitution, Title III). Section 1806(f) requires the court to determine whether the challenged surveillance was "lawfully authorized and conducted." It does not artificially limit the legal standard by which the lawfulness of the surveillance is judged only to those established by FISA. Instead, "[w]hen a district court conducts a § 1806(f) review, its task is not simply to decide whether the surveillance complied with FISA. Section 1806(f) requires the court to decide whether the surveillance was 'lawfully authorized and conducted.' " *ACLU v. Barr*, 952 F.2d 457, 465 (1991); *see also id*. at 465 n.7. In addition, section 1806(f) applies to all "materials relating to electronic surveillance." FISA defines "electronic surveillance" to encompass any "acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication . . . without the consent of any party thereto." 50 U.S.C. § 1801(f)(2). This definition of "electronic surveillance" is not limited to

foreign intelligence surveillance under FISA but includes any acquisition of a communication.

Section 1806(f) also covers communications records claims, because the "contents" of communications whose acquisition constitutes "electronic surveillance" includes "any information concerning the *identity of the parties* to such communication or the *existence* . . . of that communication." 50 U.S.C. § 1801(n) (emphasis added). Independently, information concerning disclosure of communications records is subject to section 1806(f) because such information is "material[] relating to the surveillance." § 1806(f).

D. Section 1806(f) Directs The District Court To Determine Whether Defendants Subjected Plaintiffs To Unlawful Surveillance

Section 1806(f) displaces the state secrets privilege in this lawsuit. Plaintiffs' claims all allege unlawful electronic surveillance. Plaintiffs have sought discovery of materials relating to electronic surveillance that are relevant to their claims. AER 1-6. The government informed the district court that disclosure or an adversary hearing would harm the national security of the United States when it attempted to invoke the state secrets privilege with respect to materials relating to the surveillance of plaintiffs by asserting: "Disclosure of the information covered by this privilege assertion reasonably could be expected to cause exceptionally grave damage to the national security of the United States." Dkt. # 18-3 at 3; *accord*, Dkt. # 18-4

at 3; *see also* Dkt. # 31 at 14 (government's statement that plaintiffs' discovery request (AER 1-6) "demands discovery of the very facts at issue in the privilege assertion"). Accordingly, section 1806(f) directs the district court "to determine whether surveillance 'was lawfully authorized and conducted' " (*Al-Haramain I*, 507 F.3d at 1205) with respect to each of plaintiffs' claims.[9]

The government defendants summarily assert in a footnote that section 1806(f) never preempts the state secrets privilege but decline to present any supporting argument. Gov't Defs. Br. at 38 n.11. As such, they have abandoned the issue.[10] Fed. R. App. P. 28(a)(9)(A) (appellate brief

---

[9] The government defendants' assertion that "plaintiffs do not challenge surveillance authorized by the FISA Court" (Govt. Defs. Br. at 7) misconceives both plaintiffs' complaint and the role of the district court under sections 1806(f) and 1806(h). Plaintiffs allege and challenge an untargeted mass surveillance program that violates statutory and constitutional limits on electronic surveillance. To the extent that the Government suggests that there are FISC court orders purporting to authorize the surveillance that plaintiffs allege, no such hypothetical FISC orders could satisfy the requirements of FISA or the Fourth Amendment. Regardless, it is plainly the role of the district court under sections 1806(f) and 1806(h) to review any such orders together with all other materials related to the surveillance and "determine whether the surveillance . . . was lawfully authorized and conducted," § 1806(f). Under section 1806(h), any determination that the surveillance is unlawful is binding on the FISC.

[10] The government defendants' suggestion that they could not argue the issue in this appeal is specious. By raising the state secrets privilege as an alternative ground for affirmance, the government defendants put section 1806(f)'s preemption of the state secrets privilege squarely at issue, as they well knew from the proceedings below where plaintiffs raised section

(footnote continued on following page)

must include party's "contentions and the reasons for them, with citations to the authorities and parts of the record"); *Ghahremani v. Gonzales*, 498 F.3d 993, 997 (9th Cir. 2007) (" 'Issues raised in a brief that are not supported by argument are deemed abandoned.' "); *Independent Towers of Washington v. Washington*, 350 F.3d 925, 929 (9th Cir. 2003) ("summary mention of an issue in a footnote, without reasoning in support of the [party's] argument, is insufficient to raise the issue"); *Greenwood v. FAA*, 28 F.3d 971, 977 (9th Cir. 1994) ("We review only issues which are argued specifically and distinctly in a party's opening brief. . . . We will not manufacture arguments for an appellant, and a bare assertion does not preserve a claim . . . .").

Even absent the government defendants' waiver, there is no merit to their assertion. As demonstrated above, the plain language of section 1806(f) excludes the state secrets privilege in electronic surveillance cases.

The government defendants also make a cursory argument that, even if section 1806(f) preempts the state secrets privilege, it does not apply to plaintiffs' claims. They assert that section 1806(f) applies only if the plaintiff at the pleading stage and before seeking discovery first proves both standing and a *prima facie* case on the merits, including proving that he or she is an "aggrieved person" within the meaning of FISA: "[P]laintiffs here cannot demonstrate that they are aggrieved persons within the meaning of

---

(footnote continued from preceding page)
1806(f) in opposition to the government's assertion of the state secrets privilege. Dkt. # 29 at 14-18.

FISA and thus cannot make out standing or a prima facie case on the merits." Govt. Defs. Br. at 38. "[Plaintiffs] cannot demonstrate an entitlement to proceed under FISA. Standing—and specifically, 'aggrieved person' status under FISA—must be demonstrated at the outset . . . ." *Id*.

The government defendants' argument lacks merit. It mistakenly conflates the *allegations* necessary at the pleading and discovery stage to allege standing and to state a claim with the *evidence* necessary at trial or on summary judgment to prove the allegations true. This case is at the pleading stage, and plaintiffs do not need to produce evidence proving their standing or a *prima facie* case on the merits. *See* section I(A) above.

Nor does the government defendants' argument have any basis in FISA's statutory language. Nothing in FISA requires a plaintiff to *prove* "at the outset" that they are aggrieved persons before the lawsuit can go forward.

Under FISA, an "aggrieved person" is simply "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance." 50 U.S.C. § 1801(k). Section 1810's civil remedy is available to any "aggrieved person." Congress' intent in creating the "aggrieved person" standard was to make standing to bring FISA claims "coextensive, but no broader than, those persons who have standing to raise claims under the Fourth Amendment with respect to electronic surveillance." H.R. Rep. No. 95-1283 (1978) at 66. The term was meant to exclude only "persons, not

parties to a communication, who may have been mentioned or talked about by others," because "such persons have no fourth amendment privacy right in conversations *about* them." *Id*. (emphasis added). Congress had "no intent to create a statutory right in such persons," and the purpose of the "aggrieved person" definition was simply to exclude from FISA's remedies those who were not parties to the intercepted communication. *Id*.

Section 1806(f) does not require plaintiffs to *prove* they are "aggrieved persons" who have been surveilled before it comes into play. In the text of section 1806(f), "aggrieved person" is merely a description of a person subjected to surveillance who makes a discovery request for materials relating to the surveillance. Under the Federal Rules of Civil Procedure, a plaintiff may propound discovery requests without first proving up its standing allegations or the elements of its claim. Section 1806(f) does not limit a plaintiff's right to propound discovery.

Nor is it the plaintiff's discovery request that triggers section 1806(f)'s operation. It is the government's assertion that national security evidence is at issue that triggers section 1806(f)'s directive. § 1806(f); S. Rep. No. 95-701 at 63 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4032 ("The special procedures … cannot be invoked until they are triggered by a Government affidavit that disclosure or an adversary hearing would harm the national security …. If no such assertion is made, the committee envisions … mandatory disclosure …."); FISA Conf. Rep. at 32, 1978 U.S.C.C.A.N. at 4061 (same). Without an assertion by the government that

national security evidence is at issue, discovery and trial continue along their ordinary course, evidence is disclosed, the district court determines the lawfulness of the surveillance in open proceedings, and section 1806(f) never comes into play. Because it is the government, not the plaintiff, that triggers section 1806(f), the plaintiff does not have to prove anything to trigger its operation.

The government defendants' argument that a plaintiff must not just plead but prove surveillance before section 1806(f)'s procedure comes into play is nonsensically circular. Section 1806(f) applies in cases in which an "aggrieved person" is seeking to "discover . . . materials relating to electronic surveillance." The purpose of discovery for a plaintiff is to obtain evidence needed to prove his or her claims. Discovery accordingly occurs before the plaintiff is required, either at trial or summary judgment, to put forward evidence proving his or her claims. To require instead, as the government defendants suggest, that plaintiffs first prove they have been subject to surveillance before permitting them to request discovery relating to surveillance would turn section 1806(f), and the rules of discovery, upside down.

As explained in section I, plaintiffs have satisfied their burden at the pleading stage of alleging standing for their claims. Because each plaintiff has alleged that his or her own communications and communications records were intercepted and acquired by defendants, plaintiffs have each alleged not only a concrete and particularized injury but also that they are "aggrieved

persons," i.e., "person[s] whose communications or activities were subject to electronic surveillance." 50 U.S.C. § 1801(k). They do not allege surveillance of communications to which they were *not* a party and in which they were only mentioned or talked about—the only type of surveillance excluded from the definition of "aggrieved person."[11]

Although only allegations are required at this stage, plaintiffs have more than just their allegations to show that they are aggrieved persons. There is already substantial evidence that they have been subjected to unlawful electronic surveillance. AER 8-66. For example, the Klein and Marcus declarations and AT&T's documents, which the government agrees are not state secrets, establish that the NSA has intercepted and duplicated

[11] As part of its standing analysis, the district court touched on "aggrieved person" in asserting that a plaintiff's harm could not be a concrete and particularized injury if many others suffered similar harms: "While plaintiffs . . . assert they are aggrieved, they neither allege facts nor proffer evidence sufficient to establish a prima facie case that would differentiate them from the mass of telephone and internet users in the United States and thus make their injury 'concrete and particularized' . . . ." ER 18. This is wrong on all counts. It is wrong to the extent it asserts that a plaintiff cannot be aggrieved by, and no claim for relief exists for, unlawful electronic surveillance unless it is targeted surveillance; "aggrieved person" includes both those who are "target[s] of" and those who are "subject to" surveillance. 50 U.S.C. § 1801(k). It is wrong to the extent it asserts that alleging injury in fact, or standing generally, requires stating a claim for relief. *Steel Co. v. Citizens for a Better Environment*, 523 U.S. 83, 89 (1998); *Fulfillment Services*, 528 F.3d at 619. It is wrong to the extent it asserts that to allege injury in fact a plaintiff must not just make allegations but establish a *prima facie* case. *Bennett*, 520 U.S. at 168. It is wrong to the extent it asserts that widely shared harms cannot be injuries in fact. *See* section I(C) above; AOB 16-21.

the communications transiting AT&T's communications facility in San Francisco through which plaintiffs' communications travel. *See* Appellants' RJN at Exs. A, B; *Hepting v. AT&T Corp.*, 439 F.Supp.2d 974, 989, 1001 (N.D. Cal. 2006) ("the AT&T documents and the accompanying Klein and Marcus declarations provide at least some factual basis for plaintiffs' standing" for claims arising out of the same surveillance that is at issue in this appeal).[12]

---

[12] On remand, the Al-Haramain plaintiffs amended their complaint and the district court denied the government's motion to dismiss for lack of standing, correctly noting that "*proof* of plaintiffs' claims is not necessary at this stage." *In re NSA Telcommunications Records Litigation ("Al-Haramain III")*, 595 F.Supp.2d 1077, 1085 (N.D. Cal. 2009) (emphasis original). Nevertheless, the district court's citation to *United States v. Alter*, 482 F.2d 1016 (9th Cir. 1973), might seem to suggest, contradictorily, that a plaintiff must present not just allegations of injury in fact but evidence demonstrating a *prima facie* case. *See* 595 F.Supp.2d at 1083-84. Any such suggestion, and any reliance on *Alter* for interpreting FISA, would be mistaken. *Alter* was not a section 1806(f) case but a case under 18 U.S.C. § 3504, which permits a "party aggrieved" who claims that evidence is inadmissible because it is the fruit of an illegal electronic surveillance to require the government to "affirm or deny the occurrence of" the surveillance. At the time FISA was enacted, however, it was established that a party was "aggrieved" under section 3504 so long as the party's surveillance allegations had a colorable basis. *United States v. Vielguth*, 502 F.2d 1257, 1258 (9th Cir. 1974) (section 3504 " 'is triggered . . . by the mere assertion that unlawful wiretapping has been used' "); *In re Evans*, 452 F.2d 1239, 1247 (D.C. Cir. 1971) (same); *United States v. Yanagita*, 552 F.2d 940, 943 (2d Cir. 1977) (section 3504 is triggered by surveillance allegations with a " 'colorable' basis' "). This Court had in *Vielguth* limited *Alter* to its facts, i.e., "unlawful surveillance of conversations in which [the party aggrieved] did *not* participate" (*Vielguth*, 502 F.2d at 1259 (emphasis added)), which is surveillance that falls outside of 50 U.S.C. § 1801(k)'s definition of "aggrieved person." To the extent Congress might be

(footnote continued on following page)

III. Even If Congress Had Not Preempted The State Secrets Privilege In Section 1806(f), The State Secrets Privilege Would Not Provide An Alternative Ground For Affirmance

The state secrets privilege would not provide an alternative ground for affirmance even if Congress had not preempted it in section 1806(f). The government defendants contend that the privilege excludes evidence necessary for plaintiffs to prove their claims. This assertion is incorrect, but in any event that is a determination that cannot be made at the threshold where the case stands now, but only after discovery and further proceedings. Finally, Director of National Intelligence ("DNI") Blair's privilege assertion is defective in critical respects.

A. It Is Undisputed That The "Very Subject Matter" Of This Action Is Not A State Secret And That Litigation Using Only Non-Privileged Evidence Will Not Reveal State Secrets

The decision in *Mohamed* sets forth only two circumstances in which a lawsuit may be dismissed at the threshold because it involves state secrets. The first circumstance is where the "very subject matter" of the lawsuit is a state secret. *Mohamed*, 614 F.3d at 1077-78. The government defendants do not contend that the very subject matter of this action is a state secret.

(footnote continued from preceding page)
presumed to have incorporated section 3504's jurisprudence into FISA's term "aggrieved person" (a dubious presumption given 50 U.S.C. § 1801(k)'s express definition of "aggrieved person"), it is only the "colorable basis" jurisprudence that existed in 1978 at the time of FISA's enactment that is relevant, and not *Alter*.

The second circumstance permitting threshold dismissal is where litigation of the action using only non-privileged evidence inevitably "would create an unjustifiable risk of revealing state secrets." *Mohamed*, 614 F.3d at 1088. The government defendants do not contend that "this is one of those rare cases" in which litigation of the action using only non-privileged evidence inevitably would create an unjustifiable risk of revealing state secrets. *Id*. at 1092.

Absent one of these two circumstances permitting threshold dismissal, "the effect of the government's successful invocation of privilege 'is simply that the evidence is unavailable, as though a witness had died, and the case will proceed accordingly, with no consequences save those resulting from the loss of evidence.' " *Al-Haramain I*, 507 F.3d at 1204; *accord*, *Mohamed*, 614 F.3d at 1082.

B. Whether Plaintiffs Will Be Able To Prove Their Case Using Non-Privileged Evidence Cannot Be Decided At This Stage

The government defendants argue that without privileged evidence plaintiffs will not be able to prove the merits of their case. Govt. Defs. Br. at 34 ("the cases must be dismissed because litigation of plaintiffs' claims . . . is impossible without the privileged information"), 35 ("plaintiffs cannot make out a prima facie case"). This argument, however, is one that cannot properly be evaluated at the threshold, and thus is not ripe for decision here.

A court is in no position to determine whether plaintiffs can prove up a *prima facie* case until after discovery has proceeded, the government has

asserted the state secrets privilege with respect to specific items of evidence, the court has " 'critically . . . examine[d]' " the privilege assertion as to each item of evidence, and, in instances in which it has sustained the privilege, has " 'disentangled' " privileged information from nonprivileged information. *Mohamed*, 614 F.3d at 1082. "The plaintiff's case then *goes forward* based on evidence not covered by the privilege." *Kasza*, 133 F.3d at 1166 (emphasis added). Only at that stage can the evidentiary record be established and reviewed to determine whether sufficient evidence exists for plaintiffs to prove their case. "If, *after further proceedings*, the plaintiff cannot prove the *prima facie* elements of her claim with nonprivileged evidence, then the court may dismiss her claim as it would with any plaintiff who cannot prove her case." *Id*. (emphasis added). None of these necessary steps has yet occurred in this case.

That course of proceedings is what happened in *Kasza*, which was not dismissed until after discovery had gone forward. It is what happened in *Reynolds*, where after excluding the privileged evidence the Supreme Court remanded for further proceedings to give the plaintiffs the opportunity "to adduce the essential facts as to causation without resort to material touching upon military secrets." 345 U.S. at 11. It is what happens in state secrets cases generally. *See, e.g.*, *In re Sealed Case*, 494 F.3d 139, 153 (D.C. Cir. 2007) (remanding for further proceedings); *Crater Corp. v. Lucent Technologies, Inc.*, 423 F.3d 1260, 1268-69 (Fed. Cir. 2005) (reversing dismissal because record was not sufficiently developed to determine

whether claims could proceed without the excluded state secrets evidence); *DTM Research v. AT&T*, 245 F.3d 327, 334 (4th Cir. 2001) ("the plaintiff's case should be allowed to proceed"); *Monarch Assurance P.L.C. v. United States*, 244 F.3d 1356, 1364 (Fed. Cir. 2001) (holding dismissal was "premature" because plaintiff should be "give[n] a fair amount of leeway" "in building their case from non-government sources"); *In re United States*, 872 F.2d 472, 478 (D.C. Cir. 1989) ("an item-by-item determination of privilege will amply accommodate the Government's concerns"); *Clift v. United States*, 597 F.2d 826, 827-30 (2d Cir. 1979) (reversing dismissal because plaintiff "has not conceded that without the requested documents he would be unable to proceed, however difficult it might be to do so"); *Halkin v. Helms*, 598 F.2d 1, 11 (D.C. Cir. 1978) (case remanded for further proceedings to determine whether the plaintiffs could prove some of their claims without resort to state secrets evidence). Accordingly, this Court should decline to decide at this time whether plaintiffs will be able to prove their case using nonprivileged evidence.

Even if it were proper to determine the question on this record, the government defendants' argument that it is impossible for plaintiffs to present a *prima facie* case is conclusory and abstract, divorced as it is from any reference to specific items of evidence or to the specific elements of plaintiffs' claims. Govt. Defs. Br. at 34-35. DNI Blair's privilege assertion is similarly inadequate for this purpose because it does not address specific discovery requests (including those set forth in plaintiffs' Rule 56(f)

declaration, AER 1-6) or specific items of evidence. It claims the privilege over broad categories of "information," not over specific evidence within the government's control. SER 6-10 at ¶¶ 11-19; *see Mohamed*, 614 F.3d at 1080 ("The claim also must be presented in sufficient detail for the court to make an independent determination of the validity of the claim of privilege and the scope of the evidence subject to the privilege."). In addition, the government defendants ignore the evidence already proffered by plaintiffs in this lawsuit and the related *Hepting* action demonstrating the existence of the government's dragnet, untargeted surveillance program.

The government defendants make two contentions in support of their argument that plaintiffs cannot present a *prima facie* case. First, they contend that plaintiffs will be unable to prove the injury-in-fact component of their standing. Govt. Defs. Br. at 34-35.

This contention fails. Plaintiffs have not just alleged injury in fact but have set forth an extensive factual record demonstrating interception and acquisition of their communications and communications records. AER 8-66. This record includes the Klein and Marcus declarations and associated AT&T documents establishing the NSA's dragnet interception of communications and associated communications records at AT&T's San Francisco facility through which the communications of plaintiffs, who live in the San Francisco Bay Area, pass: AT&T has installed special fiber-optic "splitters" that make a copy of every communication passing over the links between AT&T's Internet network and the Internet networks of other

telecommunications carriers and divert the copy to a secret room controlled by the NSA filled with powerful computers. Appellants' RJN, Exs. A, B; AER 21-23, 43-48. AT&T has similar installations in its facilities around the country. Appellants' RJN, Ex. A.

This is a *prima facie* showing that plaintiffs have been subjected to surveillance and therefore have suffered injury in fact. Moreover, plaintiffs are entitled to conduct additional nonprivileged discovery before they can be required to prove injury in fact.[13] *See* AER 1-6; Fed. R. Civ. P. 56(f).

The government defendants err in asserting that "the effect of the privilege is to remove *any* evidence 'that may tend to confirm or deny whether the plaintiffs have been subject to any alleged NSA intelligence activity.' " Govt. Defs. Br. at 34 (emphasis added); *id*. at 16 (privilege "removes all such evidence from the case"). The state secrets privilege removes only evidence possessed or controlled by the government and does not extend to independent evidence possessed by those, like Mark Klein, who owe no duty to the government to keep it secret. *Mohamed*, 614 F.3d at

[13] The government defendants' citation to *ACLU v. NSA*, 493 F.3d 644 (6th Cir. 2007), is unavailing. That case did not allege mass, untargeted surveillance but challenged only targeted surveillance. The plaintiffs lacked evidence that they had been parties to targeted communications and on summary judgment "concede[d] that there is no single plaintiff who can show that he or she has actually been wiretapped." *Id*. at 655. Given that concession, it was impossible for them to prove injury in fact. *Id*. at 655, 688, 691. Here, by contrast, plaintiffs allege mass, untargeted surveillance and do have evidence that their communications have been intercepted.

1090 (a "claim of privilege does not extend to public documents"). Indeed, the government has conceded not just that the Klein and Marcus declarations and the associated AT&T documents are not subject to the state secrets privilege but also that none of the subjects addressed in those documents are state secrets. Appellants' RJN, Ex. C. Thus, the government's assertion of the state secrets privilege does not preclude plaintiffs from proving the facts of the government's surveillance of them through independent evidence not obtained from the government.

The government defendants' second contention, unsupported by any reasoning or evidence, is that no matter how much nonprivileged evidence plaintiffs muster, plaintiffs cannot prove the merits of their claims without an admission from the government. Govt. Defs. Br. at 35. But " '[a]s in any lawsuit, the plaintiff may prove his case by direct or circumstantial evidence.' " *In re Sealed Case*, 494 F.3d at 147. The evidence plaintiffs already possess demonstrates the feasibility of proving their claims without an admission by the government.

Importantly, to prove their claims plaintiffs need not, and do not seek to, prove what the government defendants did with the communications and communications records they intercepted and acquired, including whatever analysis or targeting the government may or may not have subsequently applied to that mass of information. Nor are the contents of the intercepted communications and records relevant. In particular, because the statutory and constitutional violations plaintiffs allege are complete upon the

interception and acquisition of plaintiffs' own communications and records as part of a program of warrantless, untargeted, mass surveillance, plaintiffs' claims do not require them to "[i]dentify[] whether specific individuals were targets of alleged NSA activities." Govt. Defs. Br. at 7. Plaintiffs allege they were unlawfully subjected to *untargeted* surveillance and need not prove that anyone was targeted. Nor is it correct, as the government defendants and DNI Blair contend, that proving plaintiffs were subjected to mass, untargeted surveillance would reveal the identities of anyone who was targeted for surveillance. As discussed further in section III(D) below, their error lies in erroneously equating the question of whether a person was "subject to" surveillance with the altogether different question of whether a person was a "target of" surveillance. *See, e.g.*, Govt. Defs. Br. at 7, 31; SER 7-8 at ¶ 13, 19 at ¶¶ 11-12.

Moreover, it is false to assert, as the government defendants do, that "the government has not confirmed or denied the alleged activities plaintiffs seek to challenge." Govt. Defs. Br. at 35; *see also* Govt. Defs. Br. at 8 ("the government has not confirmed or denied the existence of 'dragnet' surveillance such as plaintiffs allege"), 33-34 (same). To the contrary, the government has repeatedly denied the dragnet, untargeted surveillance alleged by plaintiffs. *See* SER at 8 (DNI Blair at ¶ 14: "the NSA does not otherwise conduct a dragnet of content surveillance as the plaintiffs allege"), 20 (NSA Chief of Staff Bonnani at ¶ 13: "the NSA does not otherwise conduct the content surveillance dragnet that the plaintiffs allege");

Appellants' RJN, Ex. D (Attorney General Mukasey at ¶ 6: "the Government has denied the existence of the alleged dragnet collection on the content of plaintiffs' communications. . . . the alleged content dragnet has not occurred . . . . there was no such alleged content-dragnet"), Ex. E (NSA Director Alexander at ¶ 16: "Plaintiffs' allegations of a content surveillance dragnet are false;" at ¶ 15: "the NSA does not otherwise conduct the content surveillance dragnet that the Plaintiffs allege"); *see also* AER 66-68. Plaintiffs, of course, contest these denials, but the point is that it is not true that "disclosure of any information that might confirm or deny whether NSA conducts such [dragnet] surveillance would cause exceptionally grave harm to national security" (Govt. Defs. Br. at 34), for that disclosure has already occurred.[14]

Thus, this lawsuit cannot be dismissed on the prediction that plaintiffs will in the future be unable to prove their case with nonprivileged evidence. Instead, the case must proceed forward, " 'with no consequences save those resulting from the loss of evidence.' " *Mohamed*, 614 F.3d at 1082.

[14] The government defendants' argument, in addition to being false, also lacks logic. The government contends it would gravely harm national security to tell the American people whether or not they have been subjected en masse to untargeted surveillance, yet it tells Al Qaeda and its members and agents that it has obtained warrants subjecting them to targeted surveillance. SER 42 (NSA Director Alexander at 8 n.3).

C. The Government Defendants Have Not Proven That The Privileged Evidence Demonstrates The Existence Of A Valid Defense

The government defendants also unsuccessfully attempt to invoke the "valid-defense" exception to the principle that no party may benefit from the exclusion of state secrets evidence and litigation proceeds as though the evidence did not exist. In a single sentence unsupported by argument or explanation, they conclusorily assert that "even if plaintiffs could make out a prima facie case, the privilege would preclude defendants from presenting their defenses." Govt. Defs. Br. at 35-36. The government defendants do not identify what these purported defenses are or assert that they have submitted secret evidence *in camera* sufficient to prove the existence of these defenses.[15]

Under existing precedent, dismissal is possible in cases in which the state secrets privilege deprives a defendant of "information that would

[15] The government defendants also suggest the state secrets privilege might impinge on a hypothetical qualified immunity defense by the individual-capacity defendants. Govt. Defs. Br. at 36 n.10. The government defendants lack standing to assert qualified immunity or any other defense on behalf of the individual-capacity defendants. The individual-capacity defendants have waived the argument by declining to file any brief. The argument lacks merit in any event. When a qualified immunity motion is brought before plaintiffs have been afforded discovery, the only issue is the "purely legal" question of "whether the facts alleged . . . support a claim of violation of clearly established law." *Mitchell v. Forsyth*, 472 U.S. 511, 528 n.9 (1985). Because that issue depends only on plaintiffs' allegations, it is unaffected by any assertion of the state secrets privilege over the evidence in the case.

otherwise give the defendant a *valid* defense.' " *Mohamed*, 614 F.3d at 1083 (emphasis added) (citing *In re Sealed Case*, 494 F.3d at 153). This is a high standard to meet, and the government defendants do not even attempt to do so: "A 'valid defense' . . . is meritorious and not merely plausible and would *require* judgment for the defendant. 'Meritorious,' in turn, means 'meriting a legal victory.' " *In re Sealed Case*, 494 F.3d at 149 (citations omitted, emphasis added). To determine whether the proposed defense is meritorious and requires judgment for the defendant, the district court must examine the privileged evidence and determine whether it proves the existence of the defense: "If the defendant proffers a valid defense *that the district court verifies upon its review of state secrets evidence*, then the case must be dismissed." *Id*. at 153 (emphasis added). To avoid strategic assertions of the privilege, this verification must be especially searching when the government is not an intervenor but a defendant simultaneously withholding evidence under the privilege while seeking dismissal on the ground that it has thereby crippled itself from presenting a valid defense.

The District of Columbia Circuit has explained why the defense must be proven by the secret evidence to be "demonstrably valid" and not just "plausible:"

> Were the valid-defense exception expanded to mandate dismissal of a complaint for any plausible or colorable defense, then virtually every case in which the United States successfully invokes the state secrets privilege would need to be dismissed. This would mean abandoning the practice of deciding cases on the basis of evidence—the unprivileged

> evidence and privileged-but-dispositive evidence—in favor of a system of conjecture. . . . [I]t would be manifestly unfair to a plaintiff to impose a presumption that the defendant has a valid defense that is obscured by the privilege. There is no support for such a presumption among the other evidentiary privileges because a presumption would invariably shift the burdens of proof, something the courts may not do under the auspices of privilege.

In re Sealed Case, 494 F.3d at 149-50. The court continued: "[A]llowing the mere prospect of a privileged defense to thwart a citizen's efforts to vindicate his or her constitutional rights would run afoul of the Supreme Court's caution against precluding review of constitutional claims, see *Webster* [*v. Doe*], 486 U.S. [592,] 603-04 [(1988)], and against broadly interpreting evidentiary privileges . . . ." *In re Sealed Case*, 494 F.3d at 151.

The government has not even attempted to make the necessary showing here to trigger the valid-defense exception. It has not submitted to the district court any privileged evidence (as opposed to declarations asserting that evidence exists that is privileged). It has not identified any affirmative defense that is valid, or even one that is merely plausible.

D. The Government's Privilege Assertion Is Overbroad And Unsupported By An Adequate Showing Of Harm

For the reasons set forth above, there is no basis for affirming the district court's dismissal on the alternative ground of the state secrets privilege even if it were not the case that section 1806(f) preempts the state secrets privilege. That is not all, however.

A state secrets privilege assertion is only sustainable if it is supported by a credible showing that there is a " 'reasonable danger' " that disclosure of any of the evidence within the scope of the privilege assertion would harm national security. *Al-Haramain I*, 507 F.3d at 1196; *accord*, *Kasza*, 133 F.3d at 1170 (evaluating whether disclosure "would reasonably endanger national security"); Govt. Defs. Br. at 26 (privilege assertion requires showing that "disclosure of the information at issue would be harmful to national security"). The "critical feature of the inquiry" "is whether the *showing* of harm that might reasonably be seen to flow from disclosure is adequate in a given case to trigger the absolute right to withhold the information sought." *Halkin v. Helms*, 690 F.2d 977, 990 (1982) (emphasis original). The scope of the privilege and the asserted harm must be coextensive: To adequately support the claim of privilege, the asserted harm must be reasonably likely to occur if any of the evidence within the scope of the privilege is disclosed; otherwise, the privilege assertion is overbroad. Thus, the broader and less specific the identification of the evidence subject to the claim of privilege, the greater the showing necessary to demonstrate that disclosure of *any* of the evidence falling within the scope of the assertion is reasonably likely to harm national security. A privilege assertion can also fail if evidence within the scope of the assertion is not actually secret and has already been disclosed by the government.

DNI Blair's privilege assertion is overbroad and unsupported by an adequate showing of harm. He asserts the privilege first over "information that would reveal whether particular individuals, including the named plaintiffs in this lawsuit, have been *subject to* alleged NSA intelligence activities," i.e., untargeted dragnet surveillance, as this is the only NSA intelligence activity plaintiffs allege they have been subject to. SER 7 at ¶ 13 (emphasis added). The harm he asserts is that revealing whether plaintiffs have been "subject to" *untargeted* surveillance would reveal which individuals were or were not "*targets of*" surveillance. SER 7-8 at ¶ 13. His claim of harm lacks merit because it is a non sequitur. He erroneously equates those who are "subject to" untargeted surveillance with "targets of" surveillance by silently substituting the latter for the former from one sentence to the next. *Id*. Plaintiffs were subjected to surveillance but were not targets of surveillance because the surveillance to which they were subjected was untargeted. ER 22-44 (Complaint ¶¶ 2, 3, 7, 9, 10, 70, 74, 77-79, 82, 90, 93-95, 110, 120, 129, 138). Proving plaintiffs were unlawfully surveilled by untargeted surveillance will not involve proving that any person was a target of surveillance. Therefore, this privilege assertion fails because there is no reasonable danger that evidence of whether plaintiffs have been subject to untargeted surveillance will expose which individuals have been targets of surveillance.

DNI Blair makes an omnibus privilege assertion over "any other facts concerning NSA intelligence activities, sources, or methods that may relate

to or be necessary to litigate the plaintiffs' claims." SER 8 at ¶ 14. On its face, this assertion is meaninglessly overbroad: it has no fixed meaning because its scope is not defined by any objective criteria but simply reflexively as whatever information plaintiffs need for litigation. This simplistic "if plaintiffs need it, then it must be secret" approach is facially inadequate to define what evidence the privilege is being asserted over, much less to demonstrate that everything within this broad and amorphous description is secret and that disclosure of any of it would harm national security. *See Mohamed*, 614 F.3d at 1080 ("The claim also must be presented in sufficient detail for the court to make an independent determination of the validity of the claim of privilege and the scope of the evidence subject to the privilege."). And, of course, much of what falls within this description is not secret at all. The Inspector Generals' Report, for example, discloses much information about the NSA intelligence activities at issue here. AER 82-119. So, too, does a wealth of other evidence from government officials. *See generally* AER 16-55.

Within this overbroad privilege assertion, DNI Blair identifies three narrower subjects. The first is "facts concerning the operation of the now-inoperative Terrorist Surveillance Program." SER 8-9 at ¶¶ 14, 15. Many of these facts have been publicly disclosed by government officials. *See, e.g.*, AER 16-20, 23-28, 32-34, 38-41, 51-55, 82-119. In any event, the activities referred to as the TSP consisted of targeted surveillance activities; plaintiffs were subjected to (and their claims are limited to) untargeted surveillance.

SER 9 at ¶ 15 (TSP "directed at" al Qaeda members). Plaintiffs need not and do not intend to prove any secret "facts concerning the operation of the now-inoperative Terrorist Surveillance Program."[16] This privilege assertion is irrelevant.

The second subject is "any facts needed to demonstrate . . . that the NSA does not otherwise conduct a dragnet of content surveillance as the plaintiffs allege." SER 8-9 at ¶¶ 14, 15. Unlike DNI Blair's other privilege assertions, which cover information relating to either the existence or nonexistence of a particular fact (*id*. at ¶ 11(B) ("Information that may tend to confirm or deny"), 11(C)(ii) ("Information concerning whether or not"), 11(C)(iii) ("Information that may tend to confirm or deny")), this one deliberately is limited to facts on only one side of the coin—only facts demonstrating that the NSA does not conduct dragnet surveillance. To the extent defendants wish to use this assertion as the basis for invoking the valid-defense exception, they have failed to follow the proper procedure for doing so, as explained above. To the extent defendants make this assertion

[16] DNI Blair errs in asserting that it is "plaintiffs' allegation that the NSA has indiscriminately collected the content of millions of communications sent or received by people inside the United States after 9/11 *under the TSP*." SER 9 at ¶15 (emphasis added). By the government's own definition, the TSP is limited to targeted surveillance activities. Plaintiffs allege instead that they have been subjected to untargeted surveillance activities outside of the targeted surveillance activities denominated as the TSP.

for any other purpose, it is irrelevant; unsurprisingly, plaintiffs do not seek any evidence showing that the NSA does *not* conduct dragnet surveillance.

The third subject is "information concerning whether or not the NSA obtains transactional communications records from telecommunications companies such as AT&T." SER 8-9 at ¶¶ 14, 16. The asserted harm would come simply from "confirmation or denial" of this fact. SER 9 at ¶ 16. This fact, however, has been confirmed by numerous members of Congress "read in" to the secrets of these intelligence activities. AER 36-41. Accordingly, because this fact has already been publicly confirmed by knowledgeable government officials, no harm can come from using that same fact in litigation and the privilege assertion is moot.

DNI Blair next asserts the privilege over "information that may tend to confirm or deny whether or not AT&T (or . . . any other telecommunications provider) has assisted the NSA with alleged intelligence activities." SER 9 at ¶ 17. As the district court has already found, this information is not a secret because "public disclosures by the government and AT&T indicate that AT&T is assisting the government to implement some kind of surveillance program." *Hepting*, 439 F.Supp.2d at 994. DNI McConnell, in fact, confirmed that the telecommunications companies being sued in the *In re NSA Telecommunications* multidistrict litigation, which included AT&T, "had assisted us." AER 33. Other evidence exists as well. AER 31-41. This privilege assertion thus fails.

Finally, DNI Blair asserts the privilege over "specific information about the al-Qaeda threat." SER 10 at ¶ 18. The information covered by this privilege assertion is irrelevant to plaintiffs' claims, which are limited to untargeted surveillance and do not require proof of who was targeted for surveillance, why they were targeted, or what their connection to al Qaeda was. Nor do plaintiffs' claims require disclosure of the contents of any intercepted communications. Thus, any privilege over specific information about the al Qaeda threat is not an obstacle to litigation of plaintiffs' claims.

CONCLUSION

The judgment should be reversed and the action remanded for further proceedings.

Dated: December 6, 2010

Respectfully submitted,

s/ *Richard R. Wiebe*
RICHARD R. WIEBE
LAW OFFICE OF RICHARD R. WIEBE
One California Street, Suite 900
San Francisco, CA 94111
Telephone: (415) 433-3200
Facsimile: (415) 433-6382

CINDY A. COHN
LEE TIEN
KURT OPSAHL
KEVIN S. BANKSTON
JAMES S. TYRE
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110

Telephone: (415) 436-9333
Facsimile: (415) 436-9993

RACHAEL E. MENY
PAULA L. BLIZZARD
MICHAEL S. KWUN
AUDREY WALTON-HADLOCK
KEKER & VAN NEST LLP
710 Sansome Street
San Francisco, CA 94111
Telephone: (415) 391-5400
Facsimile: (415) 397-7188

THOMAS E. MOORE III
THE MOORE LAW GROUP
228 Hamilton Ave., 3d Fl.
Palo Alto, CA 94301
Telephone: (650) 798-5352
Facsimile: (650) 798-5001

ARAM ANTARAMIAN
LAW OFFICE OF ARAM ANTARAMIAN
1714 Blake Street
Berkeley, CA 94703
Telephone: (510) 841-2369

COUNSEL FOR PLAINTIFFS-APELLANTS

CERTIFICATE OF COMPLIANCE WITH RULE 32(a)

This brief contains 11,951 words, excluding the parts of the brief exempted by Fed. R. App. Pro. 32(a)(7)(B)(iii). Plaintiffs have concurrently filed a motion to exceed the type-volume limitations of Fed. R. App. Pro. 32(a)(7)(B) and Ninth Circuit Rule 32-1.

This brief complies with the typeface requirements of Fed. R. App. Pro. 32(a)(5) and the type style requirements of Fed. R. App. Pro. 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word in 14-point Times New Roman.

s/ *Richard R. Wiebe*

Richard R. Wiebe
Counsel for Plaintiffs-Appellants

STATUTORY APPENDIX

50 U.S.C. § 1806(f)

Appendix

50 U.S.C. § 1806(f) In camera and ex parte review by district court.

Whenever a court or other authority is notified pursuant to subsection (c) or (d), or whenever a motion is made pursuant to subsection (e), or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States of any State before any court or other authority of the United States or any state to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this Act, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, 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.