No. 06-36083
(Consolidated with Nos. 06-17132, 06-17137)

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

AL-HARAMAIN ISLAMIC FOUNDATION, INC., et al.,
Plaintiffs - Appellees,

v.

GEORGE W. BUSH, et al.,
Defendants - Appellants.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

BRIEF FOR APPELLANTS

PAUL D. CLEMENT
Solicitor General

GREGORY G. GARRE
Deputy Solicitor General

DARYL JOSEFFER
Assistant to the Solicitor General

PETER D. KEISLER
Assistant Attorney General

DOUGLAS N. LETTER
THOMAS M. BONDY
ANTHONY A. YANG
Attorneys, Appellate Staff
Civil Division, Room 7513
U.S. Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530
Telephone: (202) 514-3602

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases:

Constitution:

Statutes:

Regulations:

Legislative Materials:

Miscellaneous:

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

No. 06-36083

AL-HARAMAIN ISLAMIC FOUNDATION, INC., et al.,
Plaintiffs - Appellees,

v.

GEORGE W. BUSH, et al.,
Defendants - Appellants.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

BRIEF FOR APPELLANTS

STATEMENT OF JURISDICTION

Plaintiffs filed this action on February 28, 2006, invoking the district court's jurisdiction under 28 U.S.C. 1331. Excerpts of Record ("ER") 503. The Government moved for dismissal or summary judgment because the state secrets privilege precludes disclosure of information necessary to adjudicate the case. On September 7, 2006, the district court declined to dismiss the case and certified its order for immediate appeal under 28 U.S.C. 1292(b). On December 21, 2006, this Court granted the Government's petition for interlocutory appeal. ER 586.

STATEMENT OF THE ISSUE

Plaintiffs, a terrorist organization and two lawyers affiliated with it, contend that they were subjected to warrantless electronic surveillance under the now-discontinued Terrorist Surveillance Program ("TSP"). The district court recognized that the Government had properly invoked the state secrets privilege, and that it remains secret whether plaintiffs were actually subject to any surveillance. The question presented is whether the district court erred in nonetheless declining to dismiss the case, and instead calling for *in camera* proceedings that could risk the disclosure of state secrets.

STATEMENT OF THE CASE

Plaintiffs are Al-Haramain Islamic Foundation, Inc., an entity designated by the United States and the United Nations as a terrorist organization, and two lawyers affiliated with Al-Haramain. Plaintiffs alleged that they were subjected to warrantless foreign intelligence surveillance under the TSP, which the President authorized in the aftermath of the September 11, 2001 attacks to protect against future terrorist attacks. ER 501-08. The Government formally invoked the state secrets privilege and moved for dismissal or summary judgment because the very subject matter of this action is a state secret and the case cannot be litigated without recourse to highly classified state secrets concerning foreign intelligence gathering.

In a September 2006 ruling, the district court recognized that the Government had properly invoked the state secrets privilege, but nonetheless refused to dismiss the case. The court relied on the fact that plaintiffs had inadvertently been shown a classified document during the Treasury Department's process of designating Al-Haramain as a terrorist organization. The court found that the classified document and its contents remained a state secret, and ordered plaintiffs to return all copies of the document, but nonetheless held that plaintiffs could attempt to prove standing and a *prima facie* case, *in camera*, based on their recollection of the document's (secret) contents. ER 564-82. The court *sua sponte* certified its order for interlocutory appeal. ER 582. This Court granted interlocutory review, and subsequently consolidated this appeal with *Hepting v. AT&T Corp.*, Nos. 06-17132, 06-17137 (9th Cir.). ER 586, 599-601.

STATEMENT OF FACTS

I. The Terrorist Surveillance Program.

On September 11, 2001, al Qaeda agents who had entered the United States launched coordinated attacks on key strategic sites, killing approximately 3,000 people—the highest single-day death toll from foreign attacks in the Nation's history. The President immediately declared a national emergency in view of "the continuing and immediate threat of further attacks on the United States." 66 Fed. Reg. 48,199 (2001). The United States also launched a military campaign against al Qaeda, and

Congress authorized the President "to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks" of September 11. See Authorization for Use of Military Force ("AUMF"), Pub. L. No. 107-40, § 2(a), 115 Stat. 224 (2001). The Nation's armed forces remain engaged in a global conflict against the al Qaeda terrorist network.

The September 11 attacks demonstrated the ability of al Qaeda operatives to infiltrate the United States and murder Americans. Top al Qaeda leaders, including Osama bin Laden, have repeatedly vowed to strike America and her allies again. As the President has explained, "[t]he terrorists want to strike America again, and they hope to inflict even greater damage than they did on September the 11th." President's News Conference, 41 Weekly Comp. Pres. Doc. 1885, 1886 (Dec. 19, 2005).

Against this backdrop, and in light of unauthorized media disclosures, the President acknowledged in December 2005 that he had authorized the TSP by directing the National Security Agency ("NSA") to intercept international communications into and out of the United States of persons linked to al Qaeda. See *id.* at 1885. The Government publicly stated that communications would be intercepted under this program only if there were reasonable grounds to believe that one party to the communication was a member or agent of al Qaeda or an affiliated terrorist organization. See *id.* at 1889. The Government has never revealed the

methods and means of the TSP (including the identities of persons surveilled under the program), because of the grave harm to national security that would result from such disclosure. As discussed below, the TSP no longer exists and any surveillance that was conducted under the TSP is now subject to the approval of the FISA Court.

II. Plaintiffs' Suit And The State Secrets Privilege Assertion.

Plaintiffs are Al-Haramain Islamic Foundation, an Oregon corporation designated by the Treasury Department as a "Specially Designated Global Terrorist," and Wendell Belew and Asim Ghafoor, two attorneys with self-described "business and other relationships with plaintiff Al-Haramain." See ER 501-04. Al-Haramain's terrorist designation is based on its ties with al Qaeda and Osama bin Laden. ER 567.[1/]

In February 2006, plaintiffs filed this action in the District of Oregon against the President, the NSA, and other federal agencies and officials. Plaintiffs allege that they were subjected to warrantless electronic surveillance and that such surveillance violated the First, Fourth, and Sixth Amendments to the Constitution; the Foreign Intelligence Surveillance Act ("FISA") (50 U.S.C. 1801-1871); and the International Convention for the Suppression of the Financing of Terrorism. See ER 501-08.

[1/] Al-Haramain was designated by the Secretary of the Treasury under Executive Order 13,224, which was promulgated in part under the International Emergency Economic Powers Act. See generally *Holy Land Foundation v. Ashcroft*, 333 F.3d 156, 159-60 (D.C. Cir. 2003) (describing program).

In response, the Government asserted the state secrets privilege and related statutory privileges, and moved for dismissal or summary judgment. See Motion to Dismiss Or, In the Alternative, For Summary Judgment (June 21, 2006). The state secrets privilege, which must be invoked by the pertinent agency head, requires dismissal whenever "there is a reasonable danger" that disclosing information in court proceedings would harm national security interests, such as by disclosing intelligence-gathering methods or capabilities. See *Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998). Dismissal is required if the action's "very subject matter" is a state secret, or if the plaintiff cannot prove a *prima facie* case, or the defendant cannot establish a valid defense, without information protected by the privilege. See *ibid.*

The Government's motion was supported by public and classified declarations of the then-Director of National Intelligence, John Negroponte, and the NSA's Director, General Keith Alexander. The Government also filed public and *ex parte/in camera* briefs, explaining that it could neither confirm nor deny whether plaintiffs had been surveilled under the TSP or any other intelligence-gathering program, and that litigation of plaintiffs' claims threatened disclosure of intelligence information, sources, and methods. See Mem. In Support of Motion (June 21, 2006).

[REDACTED TEXT—PUBLIC TEXT CONTINUES ON PAGE 7]

III. The District Court's Order.

On September 7, 2006, the district court denied the Government's motion. *Al-Haramain Islamic Found., Inc. v. Bush*, 451 F. Supp. 2d 1215 (D. Or. 2006) (ER 564). Critical to the court's ruling was the fact that plaintiffs had reviewed a classified document that, they believe, shows they were surveilled. ER 572-74. As noted above, plaintiff Al-Haramain has been designated by the Treasury Secretary as a "Specially Designated Global Terrorist" for providing support to al Qaeda and Osama bin Laden, and has been similarly designated by the United Nations Security Council. Plaintiffs claim that a classified document inadvertently revealed to them during the administrative designation process shows that plaintiffs Belew and Ghafoor, and a director or directors of Al-Haramain, were subject to warrantless electronic surveillance by NSA in March and April of 2004. See ER 567-68.

The district court found that the heads of the relevant departments had properly invoked the state secrets privilege. ER 570. The court further determined that, "because the government has not officially confirmed or denied whether plaintiffs were subject to surveillance, even if plaintiffs know they were, this information remains secret." ER 572. In particular, the court held that "the Sealed Document * * * remains secret" and "contains highly classified information that must not be disclosed to the public." ER 572, 581. Accordingly, the court ordered plaintiffs to surrender their copies of the classified document (ER 578) in part because "the

government did not waive its state secrets privilege by its inadvertent disclosure of the document," ER 572. More generally, the court concluded "that whether plaintiffs were subject to surveillance" "remains secret." *Ibid.*

The court also emphasized that "plaintiffs need some information in the Sealed Document in order to establish their standing and a *prima facie* case, and they have no other available source for this information." ER 570. Instead of dismissing the case, however, the court asserted that "it is not a secret *to plaintiffs* whether [or not] their communications have been intercepted," if one accepts plaintiffs' contention that the classified document they reviewed shows that such surveillance occurred. ER 572 (emphasis added). Plaintiffs had conceded that they did not know whether any surveillance had been warrantless, and that they would need discovery to attempt to prove that they had been subject to warrantless surveillance. See 8/29/2006 Tr. 60:6-61:9. But on the theory that plaintiffs "know what information the Sealed Document contains," the court concluded that "no harm to the national security would occur if plaintiffs are able to prove the general point that they were subject to surveillance as revealed in the Sealed Document." ER 572-73. Thus, the court held that it would "permit plaintiffs to file *in camera* any affidavits attesting to the

contents of the document from their memories to support their standing in this case and to make a *prima facie* case." ER 578.[2/]

IV. The FISA Court's January 10, 2007 Orders.

While this appeal was pending, the Attorney General publicly advised the Senate Judiciary Committee that, "on January 10, 2007, a Judge of the Foreign Intelligence Surveillance Court issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that one of the communicants is a member or agent of al Qaeda or an associated terrorist organization. As a result of these orders, any electronic surveillance that was occurring as part of the Terrorist Surveillance Program will now be conducted subject to the approval of the Foreign Intelligence Surveillance Court." ER 588-89.

The Attorney General explained that, while "the [TSP] fully complies with the law," the "complex" and "innovative" FISA Court orders "will allow the necessary speed and agility while providing substantial advantages" for conducting foreign intelligence activities. *Ibid.* "[U]nder these circumstances, the President has

---

[2/] On December 15, 2006, the Judicial Panel on Multidistrict Litigation transferred this case to the Northern District of California, where it is now part of the same Multidistrict Litigation ("MDL") proceeding as the district court litigation underlying the *Hepting* appeals. See *In re NSA Telecomm. Records Litig.*, MDL No. 06-1791 (N.D. Cal.); ER 583, 587, 619.

determined not to reauthorize the Terrorist Surveillance Program when the current authorization expires." *Ibid.*

The Government subsequently submitted to the District Court for the Northern District of California public and classified declarations of General Alexander discussing the January 10 FISA Court orders. See ER 594-97 (public version).

[REDACTED TEXT—PUBLIC TEXT CONTINUES ON PAGE 11]

SUMMARY OF ARGUMENT

The district court correctly recognized that the Government has never confirmed or denied whether plaintiffs were subjected to surveillance under the TSP, and that the central premise on which plaintiffs' complaint and standing rest is therefore a secret. The district court nonetheless fundamentally erred in determining that this case could proceed by conducting *in camera* evidentiary proceedings about that state secret. Under a proper application of the Supreme Court's and this Court's state secrets cases, plaintiffs' action must be dismissed.

I. Plaintiffs' suit rests on alleged secret intelligence activities—specifically, alleged warrantless surveillance of plaintiffs undertaken as part of the TSP. It is undisputed that the Government has never publicly confirmed or denied whether the alleged surveillance took place. Moreover, the Government has formally invoked the state secrets privilege, and the public and classified declarations of the Director of National Intelligence and the Director of NSA make clear that disclosure of any information tending to confirm or deny alleged secret surveillance activities, including the specific targets of such activities, would pose a grave threat to national security. Thus, the very subject matter of this case is a state secret, and the suit must be dismissed now as a matter of law.

Plaintiffs seek to avoid the state secrets privilege by alleging that, based on their review of a classified document that was inadvertently produced to them in

connection with designating plaintiff Al-Haramain as a terrorist organization, they already know (or, more accurately, think they know) that they were subject to warrantless surveillance. The district court correctly found that "whether plaintiffs were subject to surveillance * * * remains secret," ruled that the document in question "contains highly classified information that must not be disclosed to the public," and ordered plaintiffs to return any copies of the document. ER 572, 581. But the court nonetheless concluded that this litigation could proceed by conducting evidentiary proceedings over whether the "plaintiffs were subject to [the] surveillance" that they *claim* is reflected in the document by permitting plaintiffs to submit evidence concerning what they believe or recall was in the document. ER 573.

The district court seriously erred by failing to accord the "utmost deference" to the Executive's contrary view. See *Kasza*, 133 F.3d at 1166. Moreover, the court's reasoning is fundamentally flawed in at least three ways. First, plaintiffs do not know whether their communications were intercepted, much less whether they were subjected to warrantless electronic surveillance under the TSP. Instead, plaintiffs' assertions are unsupported speculation. Indeed, plaintiffs conceded in the district court that they do not know whether any electronic surveillance of them was warrantless, or instead was authorized by the FISA Court.

Second, even if *plaintiffs* knew that one or more of them were subjected to TSP surveillance, adjudicating plaintiffs' contentions would force the Government to

inflict further harm to national security by *publicly* confirming or denying that fact. Because the Sealed Document is protected by the state secrets privilege, it necessarily follows that testimony concerning the contents of that document is protected.

Third, the district court's proposed *in camera* proceeding is fundamentally inconsistent with Supreme Court precedent requiring dismissal instead of *in camera* adjudication in order to protect state secrets. And even if an *in camera* adjudication were otherwise permissible, the district court's *decision* would reveal state secrets. A ruling in favor of plaintiffs on standing, for example, would indicate that they had been subjected to warrantless surveillance under the TSP, just as a dismissal for want of standing based on the lack of surveillance would reveal state secrets. Thus, *in camera* adjudication would be futile, as the state secrets privilege would ultimately bar the public disclosures that would be inherent in any resolution of this case.

II. Dismissal is similarly required because the state secrets privilege precludes plaintiffs from establishing, and defendants from refuting, plaintiffs' standing to sue. Plaintiffs would have standing to challenge TSP surveillance only if their own communications had been intercepted. As discussed, however, the state secrets privilege protects the TSP's methods, means, and targets—including the identities of the individuals or organizations who were surveilled. Thus, the district court correctly recognized that "plaintiffs need some information in the Sealed Document

to establish their standing." ER 570. Because that information is protected by the state secrets privilege, as discussed above, the case must be dismissed.

Plaintiffs lack standing to pursue *prospective* relief for an additional reason—they cannot prove that they are immediately in danger of *future* warrantless surveillance. As the district court recognized, because of the state secrets privilege, plaintiffs have no access to such information. Moreover, any electronic surveillance that was conducted as part of the TSP is now being conducted subject to the approval of the FISA Court. TSP surveillance is thus no longer authorized by the President or conducted by NSA. Accordingly, plaintiffs cannot show that prospective relief would redress any ongoing injury, and their claims for prospective relief must be dismissed for that reason alone. Plaintiffs' remaining claims for retrospective relief—*i.e.*, damages—cannot proceed because Congress has not waived the United States' sovereign immunity from suit for damages claims of the type asserted by plaintiffs.

III. The state secrets privilege also forecloses adjudication of the merits of plaintiffs' claims. Litigation of any of plaintiffs' claims would require detailed exploration of the nature and scope of, and the reasons for, the Government's underlying intelligence activities, including whether or not any of these activities extended to the plaintiffs, and, if so, why. As explained in the public and classified declarations, disclosure of such information would undermine national security, and any consideration of those matters would be barred by the state secrets privilege.

STANDARD OF REVIEW

This appeal raises questions of law reviewable *de novo*.

ARGUMENT

I. THE STATE SECRETS DOCTRINE REQUIRES DISMISSAL IF THE VERY SUBJECT MATTER OF A CASE IS A STATE SECRET, OR IF PLAINTIFFS CANNOT ESTABLISH A PRIMA FACIE CASE OR DEFENDANTS CANNOT MOUNT A DEFENSE WITHOUT STATE SECRETS.

The Executive's ability to protect military or state secrets from disclosure has been recognized as vital from the beginning of the Republic. See *Totten v. United States*, 92 U.S. 105, 106-07 (1875); *United States v. Reynolds*, 345 U.S. 1, 6-7 (1953). Indeed, the state secrets privilege has "a firm foundation in the Constitution, in addition to its basis in the common law of evidence," and derives from the President's Article II power over military and foreign affairs, where the "Executive's constitutional authority is at its broadest." *El-Masri v. United States*, 479 F.3d 296, 303-04 (4th Cir. 2007) (citing *United States v. Nixon*, 418 U.S. 683, 710 (1974)).

Accordingly, "the privilege to protect state secrets must head the list" of governmental privileges. *Halkin v. Helms*, 598 F.2d 1, 7 (D.C. Cir. 1978) ("*Halkin I*"). It may be invoked to protect "a broad range of information," including information that may appear innocuous on its face, but which in a larger context could reveal sensitive matters. See *Kasza*, 133 F.3d at 1166; *Halkin I*, 598 F.2d at 8. And, as here, the privilege covers sensitive information when litigation could result in

"disclosure of intelligence-gathering methods or capabilities." *Ellsberg v. Mitchell*, 709 F.2d 51, 57 (D.C. Cir. 1983) ("*Ellsberg I*").

An assertion of the state secrets privilege by a federal agency head must be "accorded the 'utmost deference' and the court's review of the privilege claim is narrow." *Kasza*, 133 F.3d at 1166. The courts must honor its assertion whenever "a reasonable danger exists that disclosing the information in court proceedings would harm national security interests." *Tenenbaum v. Simonini*, 372 F.3d 776, 777 (6th Cir. 2004); ER 569 (citing *Kasza*, 133 F.3d at 1166). "When properly invoked, the state secrets privilege is absolute. No competing public or private interest can be advanced to compel disclosure of information found to be protected by a claim of privilege." *Ellsberg I*, 709 F.2d at 57; accord *Kasza*, 133 F.3d at 1166.

Because "'public policy forbids the maintenance of any suit in a court of justice, the trial of which would inevitably lead to the disclosure of matters which the law itself regards as confidential'" (*id.* at 1170), the "state secrets privilege alone can be the basis for dismissal of an entire case." *Weston v. Lockheed Missiles & Space Co.*, 881 F.2d 814, 815-16 (9th Cir. 1989). If the "very subject matter" of the action is a state secret, the case cannot be litigated, and must be dismissed at the earliest possible stage. See *Tenet v. Doe*, 544 U.S. 1, 8-9 (2005); *Totten*, 92 U.S. at 106-07; *Kasza*, 133 F.3d at 1166, 1170. Similarly, if "the plaintiff cannot prove the *prima facie* elements of her claim with nonprivileged evidence," or the privilege "'deprives

the *defendant* of information that would otherwise give the defendant a valid defense to the claim,'" the action must be dismissed. *Kasza*, 133 F.3d at 1166. Each of those alternative bases for dismissal is present here.

II. THE VERY SUBJECT MATTER OF THIS CASE IS A STATE SECRET.

Plaintiffs' case is predicated on the allegation that the Government conducted warrantless electronic surveillance of their communications in March and April of 2004. ER 501-02 ¶¶ 1-2, 503 ¶ 19; see ER 567 & n.1. Because—as the district court itself appeared to recognize—that subject matter is itself a state secret, plaintiffs' action must be dismissed.

The district court's analysis confirms that the very subject matter of this suit is a state secret that cannot be litigated. Significantly, the district court agreed that because "whether plaintiffs were subject to surveillance * * * remains secret," the Sealed Document "contains highly classified information that must not be disclosed to the public." ER 572, 581. The court therefore accepted the Director of National Intelligence's determination to assert the state secrets privilege to "exclude [the Sealed Document] from further proceedings in this case," ER 555-56, in part because the "inadvertent disclosure of the Sealed Document does not declassify it or waive the state secrets privilege." ER 572, 577, 581. Underscoring that point, the court

ordered plaintiffs, who have no "authority * * * to review classified materials," to return "all copies" of the document. ER 578.

But the district court nevertheless displaced the judgment of the Nation's highest-ranking intelligence official by concluding that "there is no reasonable danger that the national security would be harmed" by revealing whether the "plaintiffs were subject to [the] surveillance" that they claim is reflected in the Sealed Document. ER 573. In other words, the district court agreed with the Director of National Intelligence that plaintiffs were attempting to prove a secret over which the Government had properly invoked the state secrets privilege, but rejected the Director of National Intelligence's judgment that revealing that secret would pose a reasonable danger to national security. The district court emphasized its view that "plaintiffs already know whether their communications have been intercepted," and stated that "if plaintiffs are able to prove what they allege—that the Sealed Document demonstrates they were under surveillance—no state secrets that would harm national security would be disclosed" by adjudicating this question *in camera*. ER 573, 574; see ER 572-73, 578.

That reasoning fails to accord the "utmost deference" to the Executive's view of when the disclosure of secrets will harm national security (see *Kasza*, 133 F.3d at 1166), and is fundamentally flawed in at least three ways. First, plaintiffs do not know whether their communications were actually intercepted, much less whether

they were intercepted under the TSP, as opposed to another program such as FISA. Plaintiffs' assertions are unsupported speculation, not proven facts, and forcing the Government to confirm or deny them would jeopardize national security. Second, even if *plaintiffs* knew that one or more of them had been subjected to TSP surveillance, adjudicating plaintiffs' contentions would force the Government or the court to extend the harm to national security by *publicly* confirming or denying that fact. Because the Sealed Document is protected by the state secrets privilege, it necessarily follows that testimony concerning the contents of that document is protected. Finally, the district court's proposed *in camera* proceeding—which only underscores that adjudicating this case would necessitate the disclosure of state secrets—is fundamentally inconsistent with precedents of the Supreme Court and this Court requiring dismissal instead of *in camera* adjudication in order to protect state secrets.

A. Plaintiffs Do Not Know Whether Their Communications Were Subject To Warrantless Electronic Surveillance Under The TSP.

The district court's holding is premised on its acceptance of plaintiffs' *allegation* that they already "know whether or not the government has conducted electronic surveillance of communications between" plaintiff Al-Haramain's directors and plaintiffs Belew and Ghafoor. ER 572-73 & n.3. Plaintiffs' review of a single document purportedly concerning a limited period three years ago simply does not

provide them sufficient information or context to know whether they were subjected to electronic surveillance, much less to warrantless surveillance under the TSP. Accordingly, the district court's rationale fails on its own terms.

The district court reasoned that "individuals or organizations mentioned in" a classified document would know that "their communications have been intercepted," and that, "[e]ven if plaintiffs are not identified in the document," they would "know whether their communications have been intercepted" if they had "discussed the subjects identified in the document" and "engaged in electronic communications during the period of time described in the document." ER 572. Under the district court's hypothetical situation, however, the most that could be established from such a document is that the Government acquired the names and/or information reflected in the document at some time by some means. Such a document would not by itself establish the *method* by which the Government obtained the information. But the method of acquisition may itself be of vital national security importance, and it is central to plaintiffs' case. Plaintiffs' complaint is premised on their allegation that the Government unlawfully conducted "warrantless electronic surveillance" of plaintiffs' own communications. ER 503 ¶ 18, 504 ¶ 27, 505 ¶¶ 29, 31, 506 ¶¶ 33, 35.[3/]

[3/] In this regard, this action differs from *Hepting*. The plaintiffs in *Hepting* have (continued...)

While warrantless surveillance of plaintiffs' communications might be one method of acquiring such information, there are numerous other possible means of acquiring the information relevant to the district court's analysis. For example, plaintiffs might have been surveilled under FISA—a means of court-approved surveillance that plaintiffs do not allege to be unlawful. Indeed, plaintiffs conceded in the district court that they do not know whether they were subjected to warrantless surveillance, as opposed to admittedly lawful FISA surveillance. See 8/29/2006 Tr. 60:6-61:9. Instead, plaintiffs admit that they simply "assume" that any surveillance was warrantless, based on the Government's refusal to confirm or deny whether any surveillance was court-approved. *Id.* at 96:20-97:2; see *id.* at 60:6-61:9. Yet, disclosing the particular method by which communications are intercepted (if they are intercepted at all) may disclose state secrets.

By their own admission, plaintiffs do not know whether they were subjected to warrantless surveillance under the TSP. Instead, they are attempting to draw an

---

[3/] (...continued)
now disavowed any challenge to alleged surveillance under the TSP and, instead, allege that their communications were intercepted as part of an indiscriminate "dragnet" conducted by the Government with the participation of telecommunications providers. The Government has never acknowledged the existence of any such "dragnet" program; to the contrary, the Government has denied the existence of such a program and asserted the state secrets privilege over the means, sources, and methods of the Government's foreign intelligence activities, explaining that disclosing such information would severely undermine the Nation's intelligence capabilities. See Gov't Reply Br. in *Hepting*, at 1-2.

inference from the Government's decision to invoke the state secrets privilege instead of confirming or denying whether plaintiffs were subjected to warrantless surveillance under the TSP. By relying on that inference, plaintiffs all but admit both that they lack the "knowledge" the district court considered critical and that the subject matter of this case is indeed a state secret.

Even setting FISA to the side, there are other ways the Government could become aware of communications involving one or more of the plaintiffs without surveilling the plaintiffs themselves. If Persons A and B discuss subject S in an international telephone conversation, the fact and subject matter of that conversation could be learned when B later recounts the conversation to Person C, or, alternatively, when C informs Person D that A and B discussed S. The interception of communications between B and C or between C and D would yield the same type of information in the district court's hypothetical, yet, in both instances, the communications of Person A would *not* have been intercepted.

The Government could also obtain the information relevant to the district court's analysis without conducting any surveillance at all. Person B, C, or D in the example above could voluntarily convey to the United States information about A's conversation with B. Alternatively, a foreign government that independently conducted its own surveillance of relevant communications could provide the United

States with information from that surveillance. The district court's reasoning fails to account for such plausible, alternative sources of information.

Plaintiffs' belief that they can establish that their communications were subject to the requirements of FISA at all is even more problematic. In general, FISA prohibits "electronic surveillance" except as authorized by statute (50 U.S.C. 1809(a)), and defines "electronic surveillance" to mean, in relevant part: (1) the acquisition of the contents of wire or radio communications with a device intentionally targeting a "known United States person who is *in the United States*;" (2) the acquisition of the contents of wire communications with a device where "acquisition occurs *in the United States*;" (3) the acquisition of the contents of radio communications with a device where "the sender and all intended recipients are located *within the United States*;" or (4) the installation or use of a "surveillance device *in the United States*" to acquire information other than from a wire or radio communication. See 50 U.S.C. 1801(f) (emphasis added). FISA, therefore, does not regulate all surveillance activities conducted for foreign intelligence purposes, and instead excludes many overseas intelligence activities from its scope. See H.R. Rep. No. 95-1283, at 50-51 (1978); S. Rep. No. 95-701, at 34-35 (1978). Consequently, even if one assumes that the Government itself directly obtained the content of Person A's international communication with Person B, that content could have been obtained through means other than "electronic surveillance" under FISA. Cf. Exec.

Order No. 12,333 §§ 2.2-2.5, 46 Fed. Reg. 59,941, 59,949-51 (1981) (governing overseas intelligence activities).

[REDACTED TEXT—PUBLIC TEXT CONTINUES ON PAGE 25]

B. Even If Plaintiffs Actually Knew Whether Their Communications Were Subject To Warrantless Surveillance, Litigation Would Harm National Security By Confirming Or Denying Such Alleged Surveillance.

Even putting aside plaintiffs' lack of knowledge about the alleged surveillance at issue, the district court erred in concluding that plaintiffs should be allowed to try to prove their case with evidence concerning their "memories" of the Sealed Document. ER 578. As discussed, the court correctly held that the contents of the Sealed Document are secret, and it correctly required plaintiffs to return their copies of that classified document. But the court nonetheless went on to hold that plaintiffs could try to prove those same classified facts based on their recollection of the document the court excluded from the case. In other words, the court permitted plaintiffs to attempt to proceed with evidence sketching out their recollections as to facts the court acknowledged are secret, and struck the Sealed Document itself in favor of less reliable evidence of the same classified facts.

That process effectively deprives the protected document and the protected classified information of the protection to which the district court acknowledged they were entitled under the state secrets doctrine. If plaintiffs were able to recall the contents of the Sealed Document perfectly, their evidence would constitute a mental photocopy of the privileged material. And if plaintiffs' recollection were imperfect, the accuracy of their evidence could be evaluated—or rebutted—only by referring

back to the actual contents of the document. Either way, the probative nature of plaintiffs' evidence would have to be assessed in the broader, highly classified context of foreign intelligence gathering. Thus, the very information the district court held to be secret—including the Sealed Document and its contents—would improperly be made the subject of evidentiary proceedings.

While the district court suggested that disclosure of information *to the plaintiffs* would not harm national security if plaintiffs already knew the information, the harms from confirming or denying whether plaintiffs were subjected to TSP surveillance are not limited to harms associated with plaintiffs themselves. The heads of the intelligence community and the NSA have determined that confirmation or denial of such surveillance to the *public at large* would harm national security. Both experts explained that "surveillance activities in general" are severely undermined by confirming or denying whether a particular person was surveilled because doing so would "tend to reveal intelligence information, sources, and methods that are at issue in the surveillance." ER 554, 561-62. Similarly, confirming who is not targeted for surveillance would provide insight into the scope of surveillance on a particular matter, identify for others which individuals might be a secure channel for communication, or allow identification of those targeted for surveillance in those instances where the Government declines to comment. ER 555, 562. The NSA therefore "cannot *publicly* confirm or deny whether any individual is subject to

surveillance" without harming national security with disclosures that tend to reveal intelligence targets, sources, and methods. ER 555 (emphasis added).

The courts have therefore dismissed state secrets cases even though non-governmental parties, including plaintiffs, had access to evidence concerning matters protected by the privilege. The alleged spies in *Tenet* and *Totten* had direct knowledge of facts supporting their espionage contract claims for compensation from the Government, but the Supreme Court held that the cases must be dismissed because *public* disclosure of the underlying facts would harm national security. See *Tenet*, *supra*; *Totten*, *supra*.

The plaintiff in *Sterling v. Tenet*, 416 F.3d 338 (4th Cir. 2005), *cert. denied*, 126 S. Ct. 1052 (2006), also knew his own "position and responsibilities" and the "nature of [his] duties" as a covert CIA operative, yet these matters, too, were held to "involve[] state secrets" that could not be litigated. See *id.* at 346. Similarly, the plaintiffs in *Kasza*, "who worked at [the] classified operating location" at issue there, proffered evidence based on their first-hand knowledge and other materials. Compare, *e.g.*, *Kasza*, 133 F.3d at 1162-63, 1170 & n.9, 1171-72, with *Kasza* Appellants' Brief, 1996 WL 33418896, at *18-*24. Regardless of such knowledge and evidence, this Court held that the need to discuss state secrets in order to litigate the issues in *Kasza* mandated dismissal. By the same token, even if plaintiffs here could reconstruct the contents of the Sealed Document, this action must be dismissed

because any public disclosure of the contents of the document or confirmation or denial of whether plaintiffs were subjected to surveillance under the TSP would compromise state secrets. And, because, as we have shown, plaintiffs do not know whether they have been surveilled, the harm from litigating this matter also includes confirming or denying this point to the plaintiffs.

C. The District Court's Proposed *In Camera* Procedure Would Not Adequately Protect State Secrets, And It Only Underscores The Need For Dismissal.

The district court discounted any harm from public disclosure because it contemplated a secret adjudication in which plaintiffs would attempt to prove "their standing and to make a *prima facie* case" *in camera*. See ER 578. That attempt to work around the privilege contravenes settled Supreme Court precedent. To be sure, courts may review some classified information *ex parte* and *in camera* in order to determine whether the state secrets privilege applies. ER 568. But once a court decides that information needed to adjudicate a case is protected by the privilege, dismissal is mandatory. As another court of appeals recently explained, *in camera* litigation of state secrets "is expressly foreclosed by [the Supreme Court's decision in] *Reynolds*," which "plainly held that when 'the occasion for the privilege is appropriate, * * * the court should not jeopardize the security which the privilege is meant to protect by insisting upon an examination of the evidence, *even by the judge*

alone, in chambers.'" *El-Masri*, 479 F.3d at 311 (quoting *Reynolds*, 345 U.S. at 10) (emphasis added).

The Supreme Court reaffirmed this rule in *Tenet*, explaining that, "'where the very subject matter of the action'" is "'a matter of state secret,'" the action should be dismissed at the pleading stage. *Tenet*, 544 U.S. at 9 (quoting *Reynolds*, 345 U.S. at 11 n.26). In such instances, the "use of *in camera* judicial proceedings simply cannot provide the absolute protection [the Court] found necessary in enunciating the *Totten* rule" for suits where the very subject matter of the action is a state secret. *Id.* at 11. The risk of revealing state secrets at the heart of the case—a risk inherent in conducting further judicial proceedings, even proceedings where precautions are taken to protect secrets from disclosure—is "unacceptable" as a matter of public policy. *Ibid.*; see also *Sterling*, 416 F.3d at 348. The district court's contrary approach would improperly require courts "to play with fire and chance further disclosure—inadvertent, mistaken, or even intentional—that would defeat the very purpose for which the privilege exists." *Sterling*, 416 F.3d at 344. The district court here essentially committed the same error in relying on *in camera* proceedings to circumvent the state secrets privilege that the Supreme Court corrected in *Tenet*. See *Doe v. Tenet*, 329 F.3d 1135, 1148-49 (9th Cir. 2003), *rev'd*, 544 U.S. 1 (2005).

Even if, contrary to Supreme Court precedent, an *in camera* adjudication were otherwise permissible, the district court's *decision* would reveal state secrets. A

ruling in favor of plaintiffs on standing, for example, would indicate that they had been subjected to warrantless surveillance under the TSP, just as a dismissal for want of standing based on the lack of surveillance would reveal state secrets. That a decision would reveal state secrets underscores the impropriety—and futility—of engaging in further litigation, *in camera* or otherwise. Because further litigation would "'inevitably lead to the disclosure of matters which the law itself regards as confidential,'" the case must be dismissed now. *Weinberger v. Catholic Action of Hawaii/Peace Educ. Project*, 454 U.S. 139, 147 (1981) (quoting *Totten*, 92 U.S. at 107). Further litigation would serve only to jeopardize national security by risking the disclosure of highly classified state secrets, including the disclosure of these matters to the plaintiffs themselves.

Nor does the fact that the Government publicly disclosed the existence (and subsequent termination) of the TSP alter the conclusion that this case must be dismissed. The only publicly available facts about the TSP are very general: that the TSP operated without warrants, and that it only intercepted communications that originated or concluded in a foreign country when there were reasonable grounds to believe that a party to the communication was a member or agent of al Qaeda or an affiliated terrorist organization. The Supreme Court has directed the dismissal of cases because their very subject matter was a secret even though the existence of the underlying espionage program was publicly known at some level of generality. It

was, of course, generally known that the Government hired spies during the Civil War and the Cold War, but the Court held that actions concerning the hiring of spies in those wars must be dismissed. See *Tenet, supra; Totten, supra*. There is no reason for a different result with respect to the espionage program at issue here.

III. PLAINTIFFS' STANDING CANNOT BE ESTABLISHED OR REFUTED ABSENT RECOURSE TO STATE SECRETS.

Dismissal is similarly required because plaintiffs cannot establish standing, and the Government cannot refute plaintiffs' standing, without recourse to information protected by the state secrets privilege. The district court recognized that "plaintiffs need some information in the Sealed Document to establish their standing." ER 570. Because that information is protected by the state secrets privilege, as discussed above, the case must be dismissed.

A. Plaintiffs Cannot Establish Standing Because The State Secrets Privilege Forecloses Litigation Over Whether They Have Been Subject To Warrantless Surveillance.

The Constitution "limits the jurisdiction of federal courts to 'Cases' and 'Controversies,'" and "the core component of standing is an essential and unchanging part of th[is] case-or-controversy requirement." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 559-60 (1992). To have Article III standing, a plaintiff must establish three elements—injury, causation, and redressability—and each element must not only be alleged, but proven. See *id.* at 560-61. To meet the injury requirement, a plaintiff

must show that he suffered an injury in fact to a "legally protected interest" that is "concrete and particularized" and "'actual or imminent, not 'conjectural' or 'hypothetical.'" *Id.* at 560.

A plaintiff must demonstrate Article III standing for "each claim he seeks to press," *DaimlerChrysler Corp. v. Cuno*, 126 S. Ct. 1854, 1867 (2006), and must further establish "prudential" standing by showing that "the constitutional or statutory provision on which [each] claim rests properly can be understood as granting persons in the plaintiff's position a right to judicial relief." *Warth v. Seldin*, 422 U.S. 490, 499-500 (1975). To advance a statutory claim, a plaintiff must show that his particular injury "fall[s] within 'the zone of interests to be protected or regulated by the statute'" in question. *Id.* at 683.

Courts have refused to recognize standing to challenge a Government surveillance program where the state secrets privilege prevents a plaintiff from establishing, and the Government from refuting, that he was actually surveilled. For example, in *Halkin v. Helms*, 690 F.2d 977 (D.C. Cir. 1982) ("*Halkin II*"), as here, plaintiffs claimed that Government surveillance and interception of their communications violated the Fourth Amendment in a case in which the state secrets privilege barred litigation over whether plaintiffs' communications were actually intercepted. Plaintiffs thus relied on the claim that their names were included on "watchlists" used to govern NSA surveillance, and they argued that this fact

demonstrated a "substantial threat" that their communications would be intercepted. See *id.* at 983-84, 997. The D.C. Circuit nevertheless affirmed dismissal of the Fourth Amendment claim, "hold[ing] that appellants' inability to adduce proof of actual acquisition of their communications" rendered them "incapable of making the showing necessary to establish their standing to seek relief." *Id.* at 998. As here, plaintiffs "alleged, but ultimately cannot show, a concrete injury" in light of the Government's invocation of the state secrets privilege. *Id.* at 999.

Like *Halkin* and the present case, *Ellsberg v. Mitchell* also involved a challenge to Government surveillance where the Government invoked the state secrets privilege. The D.C. Circuit again held that dismissal was warranted where a plaintiff could not, absent recourse to state secrets, establish that he was actually surveilled. As the court explained, "[a]n essential element of each plaintiff's case is proof that he himself has been injured." *Ellsberg I*, 709 F.2d at 65.

FISA likewise authorizes only an "aggrieved person" to bring a civil action challenging the acquisition of communications contents. 50 U.S.C. 1801(f), 1810. It has long been understood that "persons who [a]re not parties to unlawfully overheard conversations * * * d[o] not have standing to contest the legality of the surveillance" on Fourth Amendment grounds. *Rakas v. Illinois*, 439 U.S. 128, 136 (1978). To ensure that the term "aggrieved person" would be "coextensive [with], 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, at 66 (1978)), Congress defined "aggrieved person" to mean one "whose communications or activities were *subject to* electronic surveillance" or who was *targeted* by such surveillance. 50 U.S.C. 1801(k) (emphasis added). 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, at 89-90; cf. *United States v. Ott*, 827 F.2d 473, 475 n.1 (9th Cir. 1987); 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 discussed, the state secrets privilege precludes plaintiffs from attempting to demonstrate, and defendants from attempting to dispute, that plaintiffs' own communications were subjected to warrantless surveillance under the TSP. Accordingly, the case must be dismissed. See ER 553-55, 560-62.

[REDACTED TEXT—PUBLIC TEXT CONTINUES ON PAGE 35]

B. Plaintiffs Cannot Establish Standing To Seek Prospective Relief, And They Are Not Entitled To Money Damages.

Even assuming plaintiffs had standing to seek damages for past surveillance, and even assuming damages were available in this context, plaintiffs would lack standing to seek prospective equitable relief (see ER 507). To obtain prospective relief, it is not enough that a plaintiff allegedly suffered past injury. *City of Los Angeles v. Lyons*, 461 U.S. 95, 102 (1983); *O'Shea v. Littleton*, 414 U.S. 488, 495-96 (1974). Rather, the plaintiff must show that he is "immediately in danger of sustaining some direct injury" as the result of the challenged conduct. *Lyons*, 461 U.S. at 102.

Here, as the district court recognized, whatever is true with respect to their communications in March and April of 2004, plaintiffs certainly "do not know whether their communications continue to be intercepted" (ER 573), and, in any event, as the court also recognized, "forcing the government to confirm or deny whether plaintiffs' communications * * * continue to be intercepted * * * would create a reasonable danger that national security would be harmed by the disclosure of state secrets." *Ibid.* Accordingly, the state secrets privilege precludes any claim for relief from alleged *ongoing or future* surveillance.

Any claim for prospective relief concerning the TSP would suffer from an additional jurisdictional defect: the TSP no longer exists. The discontinuation of the

program renders plaintiffs' claim for prospective relief moot and eliminates any standing. Whether viewed as a question of standing or mootness, "'[p]ast exposure to illegal conduct does not in itself show a present case or controversy regarding injunctive [or declaratory] relief if unaccompanied by any continuing, present adverse effects.'" *Lyons*, 461 U.S. at 102. Thus, plaintiffs must "demonstrate that they are 'realistically threatened by a *repetition* of the [alleged] violation.'" *Gest v. Bradbury*, 443 F.3d 1177, 1181 (9th Cir. 2006). Here, plaintiffs cannot show any ongoing effects from the TSP because, in the wake of the FISA Court's January 2007 orders, "any electronic surveillance that was conducted as part of the TSP is now being conducted subject to the approval of the FISA Court." ER 596. TSP surveillance is no longer authorized by the President or conducted by NSA, and, accordingly, plaintiffs cannot show that prospective relief would redress any ongoing injury allegedly caused by any alleged surveillance previously conducted under the TSP.[4/]

Plaintiffs' lack of standing to pursue prospective equitable relief is especially important because they have not stated a valid damages claim. Plaintiffs rely on 50 U.S.C. 1810, but that provision does not waive the Government's sovereign

---

[4/] Wholly apart from any other issues, plaintiffs could seek declaratory and injunctive relief, at most, only with respect to alleged surveillance *of themselves*. The complaint does not seek any broader prospective relief. See ER 507 (Complaint, Prayer for Relief, ¶1) ("Plaintiffs respectfully request that the Court: 1. Declare that defendants' warrantless surveillance *of plaintiffs* is unlawful and unconstitutional, and enjoin such warrantless surveillance") (emphasis added).

immunity. Instead, it authorizes suit against "any person" as defined in 50 U.S.C. 1801(m), which does not include the United States. Congress has waived the United States' sovereign immunity against claims based on violations of some provisions of FISA, but not those at issue here. See 18 U.S.C. 2712. In any event, plaintiffs have not exhausted their administrative remedies, as required by 18 U.S.C. 2712(b)(1); cf. 28 U.S.C. 2672, 2675. Because the courts lack jurisdiction over plaintiffs' damages claims for *retrospective* relief, and plaintiffs clearly lack standing to pursue *prospective* relief, the complaint should be dismissed for that reason alone.

IV. THE STATE SECRETS PRIVILEGE ALSO PRECLUDES LITIGATION OF THE MERITS OF PLAINTIFFS' CLAIMS.

Even if the very subject matter of this litigation were not a state secret, and even if plaintiffs could prove their standing without compromising state secrets, this case should have been dismissed for another reason: plaintiffs could not prove the elements of their claims, and the Government could not defend itself against such claims, without resort to state secrets. Indeed, as with standing, the district court correctly explained that "plaintiffs need some information in the Sealed Document"—*i.e.*, information protected by the state secrets privilege, as discussed above—in order " to establish * * * a *prima facie* case." ER 570. Because plaintiffs have pursued an as-applied rather than a facial challenge, litigating this case would require disclosure not only of sensitive facts concerning the means, methods, and

subjects of surveillance under the TSP, but also of additional classified facts concerning plaintiffs themselves (including the designated terrorist organization Al-Haramain).

A. Plaintiffs' Fourth Amendment And Other Constitutional Claims.

Adjudication of plaintiffs' constitutional claims is barred by the state secrets privilege. The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const. amend. IV, cl. 1. The Amendment's "'central requirement'" is thus one of "reasonableness." *Illinois v. McArthur*, 531 U.S. 326, 330 (2001). Reasonableness is determined by assessing "'the degree to which [the search] intrudes upon an individual's privacy,'" and the "degree to which it is needed for the promotion of legitimate governmental interests" in the context of the "'totality of the circumstances'" surrounding the search. See *Samson v. California*, 126 S. Ct. 2193, 2197 (2006). Because this reasonableness inquiry depends on the nature of the search and the circumstances surrounding it, the Supreme Court has repeatedly explained that "neither a warrant, nor probable cause, nor, indeed, any measure of individualized suspicion, is an indispensable component of reasonableness in every circumstance." *National Treasury Employees Union v. Von Rabb*, 489 U.S. 656, 665 (1989) ("*NTEU*"); see *McArthur*, 531 U.S. at 330.

With respect to the TSP, at least two different exceptions to the warrant requirement are satisfied: the President's inherent authority to conduct warrantless surveillance of foreign powers, and the Fourth Amendment's "special needs" doctrine. But adjudication of either of those exceptions would require consideration of state secrets.

Consistent with the Fourth Amendment, the President has inherent constitutional authority to conduct warrantless surveillance of communications involving foreign powers such as al Qaeda and its agents. While the Supreme Court has expressly reserved that question (*United States v. U.S. District Court*, 407 U.S. 297, 308, 321-22 & n.20 (1972)), every court of appeals that has since decided it has held that the President possesses "inherent authority" under the Constitution, not trumped by the Fourth Amendment, "to conduct warrantless searches to obtain foreign intelligence information." *In re Sealed Case*, 310 F.3d 717, 742 & n.26 (FIS Ct. of Rev. 2002); accord *United States v. Buck*, 548 F.2d 871, 875-76 (9th Cir. 1977); *United States v. Truong*, 629 F.2d 908, 912-17 (4th Cir. 1980); *United States v. Butenko*, 494 F.2d 593, 602-06 (3d Cir. 1974); *United States v. Brown*, 484 F.2d 418, 425-26 (5th Cir. 1973). Indeed, this proposition is now so firmly entrenched that the Foreign Intelligence Surveillance Court of Review—the appellate tribunal charged with reviewing FISA Court decisions—took "for granted that the President does have that authority." *In re Sealed Case*, 310 F.3d at 742.

Under the foreign intelligence doctrine, warrantless searches are reasonable if conducted to secure foreign intelligence information. See *Truong*, 629 F.2d at 916-17; *Butenko*, 494 F.2d at 606; *Brown*, 484 F.2d at 421, 425. Inquiry into the facts surrounding a decision to conduct TSP surveillance, however, would necessarily confront the state secrets privilege. As discussed, facts concerning the program's "intelligence activities, sources, methods, or targets" can neither be confirmed nor denied. ER 554; see ER 561. The D.C. Circuit concluded in analogous circumstances that the "notion of deciding [the] constitutional question" of "whether a warrant is required in certain foreign intelligence surveillances, and if not, whether certain activities are 'reasonable'" when the "record [is] devoid of any details that might serve even to identify the alleged victim of a violation," is not only "impossible," but "ludicrous." *Halkin II*, 690 F.2d at 1000, 1003 n.96.

The "special needs" doctrine independently supports the validity of the TSP. "[W]here a Fourth Amendment intrusion serves special governmental needs, beyond the normal need for law enforcement, it is necessary to balance the individual's privacy expectations against the Government's interests to determine whether it is impractical to require a warrant or some level of individualized suspicion in the particular context." *NTEU*, 489 U.S. at 665-66. The "special needs" doctrine applies in "a variety of contexts," including warrantless searches used to detect and prevent drunk driving, drug use by students and federal officials, airline hijackings, and

terrorist bombings. See, *e.g.*, *MacWade v. Kelly*, 460 F.3d 260, 263, 268 (2d Cir. 2006); *Board of Educ. v. Earls*, 536 U.S. 822, 835-36 (2002); *City of Indianapolis v. Edmond*, 531 U.S. 32, 44 (2000). It is "settled" that the Government's need to "discover" and "prevent the development of hazardous conditions" can qualify as a special need justifying warrantless and suspicionless searches. See *NTEU*, 489 U.S. at 668.

In applying the "special needs" doctrine, reasonableness is determined by conducting a "fact-specific balancing" of the Government interests underlying the search and the associated intrusion into privacy interests. See *Earls*, 536 U.S. at 830. Again, the state secrets privilege protects the information required for this fact-specific inquiry, such as information concerning the nature of the al Qaeda threat; facts supporting the need for speed and flexibility in conducting surveillance beyond that traditionally available under the FISA; details concerning the TSP's targeting decisions, effectiveness in detecting and preventing terrorist attacks, and other operational information; and other specifics concerning the scope and nature of TSP surveillance. See ER 553-56, 560-62. Application of the special needs doctrine therefore cannot properly be adjudicated in light of the state secrets privilege. Nor is there any reason to suppose that plaintiffs' First and Sixth Amendment claims are less fact-dependent than their Fourth Amendment claim.

[REDACTED TEXT—PUBLIC TEXT CONTINUES ON PAGE 42]

B. Plaintiffs' FISA Claim.

Plaintiffs' FISA claim (see ER 504-05) fares no better. A violation of FISA occurs if a person "intentionally—(1) engages in electronic surveillance under color of law except as authorized by statute; or (2) discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by statute." 50 U.S.C. 1809(a). Plaintiffs could not show that the TSP's activities qualified as "electronic surveillance" (see 50 U.S.C. 1801(f)) without delving into state secrets concerning the means, methods, and targets of surveillance under the TSP. Moreover, even if plaintiffs could establish that the activities at issue otherwise fell within the scope of FISA, their claim that FISA precluded TSP surveillance—thereby constraining the President's ability to collect surveillance of a foreign enemy during wartime—raises a grave constitutional question, the proper resolution of which would necessarily require consideration of matters protected by the state secrets privilege.

In wartime, the "President alone" is "constitutionally invested with the entire charge of hostile operations." *Hamilton v. Dillin*, 88 U.S. 73, 87 (1874). Congress may not "interfere[] with the command of the forces and the conduct of campaigns" because that "power and duty belong to the President as commander-in-chief." *Ex parte Milligan*, 71 U.S. 2, 139 (1866) (Chase, C.J., concurring). The President's

Commander-in-Chief powers include secretly gathering intelligence information about foreign enemies. See, *e.g.*, *Totten*, 92 U.S. at 106; *Chicago & S. Air Lines v. Waterman S.S. Corp.*, 333 U.S. 103, 111 (1948); *United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 320 (1936). As discussed, every court of appeals to have decided the question has held that, even in peacetime, the President has inherent constitutional authority to conduct warrantless surveillance of foreign powers within or without the United States. See pp. 39-40, *supra*.

Congress may not "impede the President's ability to perform his constitutional duty." *Morrison v. Olson*, 487 U.S. 654, 691 (1988); see *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 637-38 (1952) (Jackson, J., concurring). The Constitution designates the President as Commander-in-Chief, U.S. Const., art. II, § 2, and "the object of the [Commander-in-Chief Clause] is evidently to vest in the [P]resident * * * such supreme and undivided command as would be necessary to the prosecution of a successful war." *United States v. Sweeny*, 157 U.S. 281, 284 (1895). In the context of the current conflict with al Qaeda—a foreign enemy that has already attacked the United States—the President and his top advisors determined in the aftermath of September 11 that the threat to the United States demanded that signals intelligence be carried out with a speed and methodology that could not be achieved by seeking judicial approval through the traditional FISA process (but which is now occurring subject to the recent, innovative orders of the FISA Court).

Moreover, the President's constitutional prerogative to engage in surveillance directed at al Qaeda is reinforced by Congress's Authorization for Use of Military Force (see pp. 3-4, *supra*), which recognized the President's "authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States," and explicitly authorized the President to act against those responsible for the attacks of September 11, 2001. See AUMF pmbl., § 2(a). The President's ability to "deter and prevent acts of international terrorism against the United States," as well as to detect and apprehend the individuals and organizations responsible for the September 11 attacks, necessarily is dependent on his ability to engage in foreign intelligence gathering.

For present purposes, the crucial point is that FISA must be construed in light of the President's constitutional authority in this realm, and the constitutionality of any limits placed on the President's authority to gather foreign intelligence against the enemy in wartime cannot be measured without a precise understanding of the program at issue and the threat it is designed to address. That inquiry would require careful consideration of the nature and scope of the surveillance in question, as well as the precise nature of the existing al Qaeda threat, including an examination of the scope, targets, methods, and means of surveillance directed against that threat. As

discussed above, however, the facts relevant to that inquiry are protected from disclosure by the state secrets privilege.[5/]

CONCLUSION

For the foregoing reasons, the district court's decision should be reversed and this case dismissed.

Respectfully submitted,

PAUL D. CLEMENT
Solicitor General

GREGORY G. GARRE
Deputy Solicitor General

DARYL JOSEFFER
Assistant to the Solicitor General

PETER D. KEISLER
Assistant Attorney General

DOUGLAS N. LETTER
THOMAS M. BONDY
ANTHONY A. YANG
Attorneys, Appellate Staff
Civil Division, Room 7513
U.S. Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530
Telephone: (202) 514-3602

JUNE 2007

[5/] Plaintiffs' claim under the International Convention for the Suppression of the Financing of Terrorism must be dismissed for similar reasons, even assuming *arguendo* that plaintiffs have a private right of action to sue the Government for alleged violations of the Convention. See, *e.g.*, *Iguarta-De La Rosa v. United States*, 417 F.3d 145, 150 (1st Cir. 2005) (en banc), *cert. denied*, 126 S. Ct. 1569 (2006); *Diggs v. Richardson*, 555 F.2d 848, 850 (D.C. Cir. 1976). Insofar as plaintiffs also seek to raise an "expunction" claim (see ER 507), dismissal of that claim is compelled on the same grounds.

STATEMENT OF RELATED CASES

As noted above, this Court has consolidated this appeal with *Hepting v. AT&T Corp.*, Nos. 06-17132, 06-17137 (9th Cir.).

ADDENDUM

ADDENDUM TABLE OF CONTENTS

Page

U.S. Constitution, Amend. IV

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Authorization for Use of Military Force, preamble, § 2(a)

Whereas, on September 11, 2001, acts of treacherous violence were committed against the United States and its citizens; and

Whereas, such acts render it both necessary and appropriate that the United States exercise its rights to self-defense and to protect United States citizens both at home and abroad; and

Whereas, in light of the threat to the national security and foreign policy of the United States posed by these grave acts of violence; and

Whereas, such acts continue to pose an unusual and extraordinary threat to the national security and foreign policy of the United States; and

Whereas, the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States: Now, therefore, be it

Resolved by the Senate and House of Representatives of the United States of America in Congress assembled,

* * * *

SEC. 2. AUTHORIZATION FOR USE OF UNITED STATES ARMED FORCES.

(a) IN GENERAL.—That the President is authorized to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons.

* * * *

Foreign Intelligence Surveillance Act of 1978, as amended
50 U.S.C. 1801-1871

50 U.S.C. 1801

§ 1801. Definitions

As used in this subchapter:

* * * *

(f) "Electronic surveillance" means--

(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18;

(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

* * * *

(k) "Aggrieved person" means a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.

* * * *

(m) "Person" means any individual, including any officer or employee of the Federal Government, or any group, entity, association, corporation, or foreign power.

* * * *

50 U.S.C. 1809

§ 1809. Criminal sanctions

(a) Prohibited activities

A person is guilty of an offense if he intentionally--

(1) engages in electronic surveillance under color of law except as authorized by statute; or

(2) discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by statute.

* * * *

50 U.S.C. 1810

§ 1810. Civil liability

An aggrieved person, other than a foreign power or an agent of a foreign power, as defined in section 1801(a) or (b)(1)(A) of this title, respectively, who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 1809 of this title shall have a cause of action against any person who committed such violation and shall be entitled to recover--

(a) actual damages, but not less than liquidated damages of $1,000 or $100 per day for each day of violation, whichever is greater;

(b) punitive damages; and

(c) reasonable attorney's fees and other investigation and litigation costs reasonably incurred.

Title 18, United States Code

18 U.S.C. 2712

§ 2712. Civil actions against the United States

(a) In general.--Any person who is aggrieved by any willful violation of this chapter or of chapter 119 of this title or of sections 106(a), 305(a), or 405(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U. S.C. 1801 et seq.) may commence an action in United States District Court against the United States to recover money damages. In any such action, if a person who is aggrieved successfully establishes such a violation of this chapter or of chapter 119 of this title or of the above specific provisions of title 50, the Court may assess as damages--

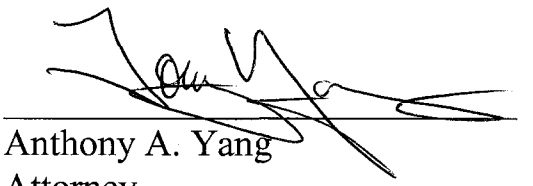
(1) actual damages, but not less than $10,000, whichever amount is greater; and
(2) litigation costs, reasonably incurred.

(b) Procedures.--(1) Any action against the United States under this section may be commenced only after a claim is presented to the appropriate department or agency under the procedures of the Federal Tort Claims Act, as set forth in title 28, United States Code.

* * * *

CERTIFICATE OF COMPLIANCE

I hereby certify that this brief is in compliance with Rule 32(a)(7) of the Federal Rules of Appellate Procedure. The public and classified versions of this brief contain no more than 14,000 words, and were prepared in 14-point Times New Roman font using Corel WordPerfect 12.0.



Anthony A. Yang
Attorney

CERTIFICATE OF SERVICE

I certify that on this 6th day of June, 2007, I dispatched the foregoing by Federal Express and electronic mail to the following counsel:

Counsel for Plaintiffs-Appellees:

– via Federal Express & electronic mail:

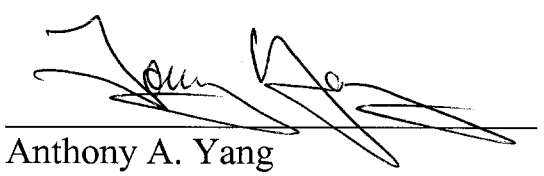
Jon B. Eisenberg, Esq.
Eisenberg & Hancock, LLP
1970 Broadway, Suite 1200
Oakland, CA 94612
510-452-2581
jon@eandhlaw.com

– via electronic mail only:

Lisa R. Jaskol, Esq. (ljaskol@publiccounsel.org)
Steven Goldberg, Esq. (steven@stevengoldberglaw.com)
Thomas H. Nelson, Esq. (nelson@thnelson.com)
Zaha S. Hassan, Esq. (zahahassan@comcast.net)
J. Ashlee Albies, Esq. (ashlee@albieslaw.com)

Counsel for Intervenor (via electronic mail only):

Charles F. Hinkle, Esq.
Emilie K. Edling, Esq.
Stoel Rives, LLP
900 SW Fifth Avenue, Suite 2600
Portland, OR 97204
cfhinkle@stoel.com; ekedling@stoel.com



Anthony A. Yang
Attorney