



Case Western Reserve Journal of International Law

Volume 42 | Issue 3

2010

Litigating the State Secrets Privilege

Lee Tien

Follow this and additional works at: <https://scholarlycommons.law.case.edu/jil>



Part of the [International Law Commons](#)

Recommended Citation

Lee Tien, *Litigating the State Secrets Privilege*, 42 Case W. Res. J. Int'l L. 675 (2010)

Available at: <https://scholarlycommons.law.case.edu/jil/vol42/iss3/8>

This Article is brought to you for free and open access by the Student Journals at Case Western Reserve University School of Law Scholarly Commons. It has been accepted for inclusion in Case Western Reserve Journal of International Law by an authorized administrator of Case Western Reserve University School of Law Scholarly Commons.

LITIGATING THE STATE SECRETS PRIVILEGE

Lee Tien^{*}

The state secrets privilege raises important separation of powers and institutional competence questions, especially for courts. Congress can statutorily modify this common-law evidentiary privilege, which should facilitate judicial management of civil litigation with national security implications. Under the Foreign Intelligence Surveillance Act, for example, district courts are expressly authorized to evaluate the legality of government electronic surveillance in special proceedings. This article describes some of the practical litigation problems that arise even when Congress authorizes courts to review claimed national security secrets in the context of a case alleging that the National Security Agency engaged in unlawful warrantless wire-tapping.[†]

I. INTRODUCTION

Much has been written about the constitutional issues raised by the Executive's use of the state secrets privilege to frustrate civil litigation over

^{*} Senior Staff Attorney, Electronic Frontier Foundation. Thanks to Jon Eisenberg and Ashlee Albies for their very helpful comments.

[†] As this article went to press, Judge Walker granted summary judgment to the Al-Haramain plaintiffs, finding that the government had violated the Foreign Intelligence Surveillance Act (FISA). *In re Nat'l Sec. Agency Telecomm. Records Litig.*, F. Supp. 2d, 2010 WL 1244349 (N.D. Cal. Mar. 31, 2010). The court was dismissive of the government's claim of unbridled Executive power: "Under defendants' theory, executive branch officials may treat FISA as optional and freely employ the SSP [state secrets privilege] to evade FISA, a statute enacted specifically to rein in and create a judicial check for executive branch abuses of surveillance authority." *Id.* at *13. The government had steadfastly refused to engage the Al-Haramain plaintiffs on the facts, as discussed more fully in this article. Accordingly, the court found that "defendants could readily have availed themselves of the court's processes to present a single, case-dispositive item of evidence at one of a number of stages of this multi-year litigation: a FISA warrant. They never did so." *Id.* at *14. Therefore, "[f]or purposes of this litigation, there was no such warrant for the electronic surveillance of any of plaintiffs," and the surveillance therefore violated FISA. *Id.* at *15. Aside from finding the government liable for violating FISA and dismissing all claims against FBI Director Robert Mueller in his individual capacity, the decision did not resolve any of the Al-Haramain plaintiffs' other legal claims. *See id.* at *21. Judge Walker gave them a choice: voluntarily dismiss their non-FISA claims and obtain a final judgment, including damages, on their FISA claim, or press their additional claims, in which case the court and the parties would schedule a case management conference to determine further proceedings. *Id.*

violations of statutory and constitutional rights.¹ However, the epic nature of the theoretical issues of separation of powers and individual rights in the national security context should not distract us from the practical impact of state secrets privilege assertions on litigation even after the case survives multiple motions to dismiss. How are plaintiffs to litigate cases when courts fear that the litigation itself may touch upon state secrets that may, if disclosed, harm national security?

The Supreme Court seemed to answer this question in the seminal state secrets case *United States v. Reynolds*,² which concerned a tort action for wrongful death arising out of a military airplane crash. Although the Supreme Court found that evidence about electronic devices that were being tested when the plane crashed and killed the plaintiffs' spouses was indeed protected by the state secrets privilege,³ it nevertheless remanded the case to proceed without the privileged materials.⁴ The Court noted that because the surviving crew members were available for examination, "it should be possible for [the plaintiffs] to adduce the essential facts as to causation without resort to material touching upon military secrets."⁵

Reynolds thus expresses confidence that courts and plaintiffs can manage discovery even when state secrets are involved. Courts nevertheless continue to be perplexed by the actual management of state secrets cases. The Executive's demand that courts "look down the road"—i.e., to evaluate a case far in advance of the normal procedures for developing an evidentiary record—runs contrary to the iterative fact-development process of normal litigation and forces courts to play litigation gatekeeper in difficult circumstances. Even when courts find a reasonable path to navigate, they face practical difficulties in making the normal adversary process work in the face of Executive refusal to provide litigants or their counsel with access to information needed to litigate the case.

¹ See, e.g., Amanda Frost, *The State Secrets Privilege and Separation of Powers*, 75 FORDHAM L. REV. 1931 (2007); Heidi Kitrosser, *Secrecy and Separated Powers: Executive Privilege Revisited*, 92 IOWA L. REV. 489 (2007); Robert M. Chesney, *State Secrets and the Limits of National Security Litigation*, 75 GEO. WASH. L. REV. 1249 (2007); D. A. Jeremy Telman, *Our Very Privileged Executive: Why the Judiciary Can (and Should) Fix the State Secrets Privilege*, 80 TEMP. L. REV. 499 (2007); William G. Weaver & Robert M. Pallitto, *State Secrets and Executive Power*, 120 POL. SCI. Q. 85, 108–32 (2005); Christina E. Wells, *State Secrets & Executive Accountability*, CONST. COMMENT. (forthcoming 2010), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1576578; Laura Donohue, *The Shadow of State Secrets*, 159 U. PA. L. REV. (forthcoming 2010), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1566982.

² 345 U.S. 1 (1953).

³ *Id.* at 10–11.

⁴ *Id.* at 12.

⁵ *Id.* at 11.

This article tells a cautionary tale of how the Executive refused to accept judicial authority to manage litigation and to grant some level of litigant access in the interests of due process and the federal courts' Article III power to decide cases. Courts and litigants face significant hurdles in actual litigation even when Congress has preempted the state secrets privilege so as to avoid threshold dismissal.

II. BACKGROUND ON THE STATE SECRETS PRIVILEGE AND THRESHOLD DISMISSAL

The state secrets privilege prevents discovery of secret evidence when disclosure would threaten national security. *Reynolds* set forth the basic framework of the privilege: (1) it belongs to the government; (2) it must be properly invoked by means of a "formal claim of privilege, lodged by the head of the department which has control over the matter" after "actual personal consideration;"⁶ (3) the court must then "determine whether the circumstances are appropriate for the claim of privilege, and yet do so without forcing a disclosure of the very thing the privilege is designed to protect;"⁷ (4) the precise nature, extent, and manner of this inquiry depends in part on the extent of a party's need for the information sought tested against the strength of the government's claim of privilege;⁸ and (5) *in camera* review can be appropriate, but not in all cases.⁹

When the privilege applies, "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 the evidence," and with "no alteration of pertinent substantive or procedural rules."¹⁰ Two of these consequences are relatively clear. Litigation may proceed so long as (1) the plaintiffs can still prove "the essential facts" of their claims;¹¹ and (2) invocation of the privilege does not deprive "the defendant of information that would otherwise give the defendant a valid defense."¹² Otherwise, the case may be dismissed or summary judgment may be granted for the defendant.¹³

⁶ *Id.* at 8.

⁷ *Id.* (citation omitted).

⁸ *Id.* at 11.

⁹ *See id.* at 10.

¹⁰ *Ellsberg v. Mitchell*, 709 F.2d 51, 64 (D.C. Cir. 1983) (citations omitted); *see id.* at 65 (remanding to determine whether plaintiffs could prove prima facie case without privileged information).

¹¹ *See Reynolds*, 345 U.S. at 11.

¹² *Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998) (quoting *Bareford v. General Dynamics Corp.*, 973 F.2d 1138, 1141 (5th Cir. 1992)). A "valid defense" is "meritorious and not merely plausible and would require judgment for the defendant." *In re Sealed Case*, 494 F.3d 139, 149–50 (D.C. Cir. 2007) ("Were the valid-defense exception expanded to mandate dismissal of a complaint for any plausible or colorable defense, then virtually every

More controversial is the third possible consequence: if the “very subject matter of the action is a state secret,” courts often dismiss the plaintiff’s action based solely on the invocation of the state secrets privilege.¹⁴ In *Mohamed v. Jeppesen Dataplan*,¹⁵ which challenged the Central Intelligence Agency’s extraordinary rendition program, the Ninth Circuit held that this type of threshold dismissal is not available under *Reynolds* because “[t]his sweeping characterization of the ‘very subject matter’ bar has no logical limit” and would “cordon off all secret government actions from judicial scrutiny.”¹⁶ Instead, the proper course is to “excis[e] secret evidence on an item-by-item basis, rather than foreclos[e] litigation altogether at the outset.”¹⁷ The case is being reheard *en banc* and under submission as of this writing.¹⁸

III. LITIGATION OVER THE WARRANTLESS SURVEILLANCE PROGRAM

A. Background

On December 16, 2005, the *New York Times* reported that in the years following September 11, 2001, President Bush secretly authorized the National Security Agency (NSA) to conduct electronic surveillance on Americans and others without warrants.¹⁹ The Government soon publicly acknowledged that its secret activities had indeed included the warrantless interception of international communications where one party to the communication was believed to have links to al-Qaeda and related terrorist organizations.²⁰

case in which the United States successfully invokes the state secrets privilege would need to be dismissed.”).

¹³ See, e.g., *Molerio v. FBI*, 749 F.2d 815, 826 (D.C. Cir. 1984) (granting summary judgment where the state secret privilege precluded the government from using a valid defense).

¹⁴ *Kasza*, 133 F.3d at 1166 (quoting *Reynolds*, 345 U.S. at 11 n.26).

¹⁵ *Mohamed v. Jeppesen Dataplan, Inc.*, 579 F.3d 943, 949 (9th Cir. 2009).

¹⁶ *Id.* at 955. Threshold dismissal for lawsuits brought by plaintiffs on the basis of secret espionage agreements with the Government remains viable under the separate doctrine of *Totten v. United States*, 92 U.S. 105 (1876). *Mohamed*, 579 F.3d at 954 (noting that under *Tenet v. Doe*, 544 U.S. 1, 10 (2005), *Totten* prohibits only suits that would necessarily reveal “the plaintiff’s [secret] relationship with the Government”).

¹⁷ *Mohamed*, 579 F.3d at 995.

¹⁸ *Mohamed v. Jeppesen Dataplan, Inc.*, 586 F.3d 1108 (9th Cir. 2009).

¹⁹ James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

²⁰ OFFICE OF INSPECTOR GEN. OF THE DEP’T OF DEF. ET AL., UNCLASSIFIED REPORT ON THE PRESIDENT’S SURVEILLANCE PROGRAM 6 (July 10, 2009), available at <http://www.justice.gov/oig/special/s0907.pdf>. While the surveillance acknowledged in December 2005 is known as the “Terrorist Surveillance Program,” the report of the Inspector General makes clear that the President also authorized “Other Intelligence Activities.” *Id.* (citing Letter from Alberto

On May 11, 2006, *USA Today* reported the existence of an NSA program in which some telecommunications carriers were alleged to have provided telephone calling records of tens of millions of Americans to the NSA.²¹ The article alleged that BellSouth Corp., Verizon Communications Inc., and AT&T gave the government access to a database of domestic communication records that the NSA uses “to analyze calling patterns in an effort to detect terrorist activity.”²²

In response to these revelations:

[D]ozens of lawsuits by customers of telecommunications companies were filed alleging various causes of action related to such cooperation with the NSA in warrantless wiretapping of customers’ communications. . . . The cases typically alleged federal constitutional and statutory violations as well as causes of action based on state law such as breach of contract, breach of warranty, violation of privacy and unfair business practices.²³

The Judicial Panel on Multidistrict Litigation ordered these cases transferred to the Northern District of California in August 2006 and consolidated before U.S. District Judge Vaughn Walker.²⁴

These cases against the telecommunications companies followed a common pattern.

The United States moved to intervene in the case and simultaneously to dismiss it, asserting the state secrets privilege (SSP) and arguing, in essence, that the SSP required immediate dismissal because no further progress in the litigation was possible without compromising national security. The telecommunications company defendants in the case also moved to dismiss on other grounds.²⁵

Gonzales, U.S. Attorney General, to Senator Patrick Leahy, Chairman, Committee on the Judiciary (Aug. 1, 2007), *available at* <http://ftp.fas.org/irp/news/2007/08/ag080107.pdf> (“The specific details of the Other Intelligence Activities remain highly classified, although the Attorney General publicly acknowledged the existence of such activities in August 2007. Together, the Terrorist Surveillance Program and the Other Intelligence Activities comprise the PSP.”).

²¹ Leslie Cauley, *NSA Has Massive Database of Americans’ Phone Calls*, USA TODAY, May 11, 2006, at 1A.

²² *Id.*

²³ *In re Nat’l Sec. Agency Telecomm. Records Litig.*, 633 F. Supp. 2d 949, 955 (N.D. Ca. 2009) (dismissing cases against telecommunications carrier defendants), *appeal pending* No. 09-16676 (9th Cir.). The basis for the dismissal was the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FISAAA). *See infra* note 27 and accompanying text.

²⁴ *In re Nat’l Sec. Agency Telecomm. Records Litig.*, 633 F. Supp. 2d at 956.

²⁵ *Id.* at 955–56 (citations omitted).

In the first of these cases, decided prior to the MDL transfer, the district court denied the motions to dismiss.²⁶ All of the cases were eventually dismissed, however, based on section 802 of the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FISAAA),²⁷ which “included an immunity provision for the benefit of telecommunications companies that would be triggered if and when the Attorney General of the United States certified certain facts to the relevant United States district court.”²⁸

B. The Al-Haramain Case

While most of these cases were brought against the telecommunications companies themselves, some were brought against the Government and individual government officials.²⁹ The most notable of these cases was brought by the Al-Haramain Islamic Foundation³⁰ and two of its individual attorneys, Wendell Belew and Asim Ghafoor.³¹

²⁶ See *Hepting v. AT&T Corp.*, 439 F. Supp. 2d 974 (N.D. Cal. 2006).

²⁷ Pub. L. No. 110-261, 122 Stat. 2436 (codified at 50 U.S.C. § 1885a); see *In re Nat'l Sec. Agency Telecomm. Records Litig.*, 633 F. Supp. 2d at 956–60 (N.D. Cal. 2009) (discussing immunity provisions).

²⁸ See *In re Nat'l Sec. Agency Telecomm. Records Litig.*, 633 F. Supp. 2d at 956. FISAAA was enacted while *Hepting* was first on appeal to the Ninth Circuit, which remanded the case without rendering a decision “in light of the FISA Amendments Act of 2008.” *Hepting v. AT&T Corp.*, 539 F.3d 1157 (9th Cir. 2008).

²⁹ See, e.g., *Ctr. for Constitutional Rights v. Bush*, No. C 07-1115 (VRW) (N.D. Cal. Feb. 23, 2007); *Guzzi v. Bush*, No. C 06-6225 (VRW) (N.D. Cal. Oct. 3, 2006), *dismissed per stipulation*, Order, *In re Nat'l Sec. Agency Telecomm. Records Litig.*, No. 06-1791 (VRW) (N.D. Cal. Mar. 5, 2010), available at <http://docs.justia.com/cases/federal/district-courts/california/candce/M:2006cv01791/183077/713/>; *Shubert v. Bush*, No. C 07-0693 (VRW), 2010 WL 235075 (N.D. Cal. Jan. 21, 2010) (dismissing *Shubert*); *Jewel v. Nat'l Sec. Agency*, No. C 08-4373 (VRW), 2010 WL 235075 (N.D. Cal. Jan. 21, 2010) (dismissing *Jewel*). In addition, some cases were brought by the U.S. “seeking to enjoin state officials in Maine, New Jersey, Connecticut, Vermont and Missouri from investigating various telecommunication carriers concerning their alleged disclosure of customer telephone records” to the NSA. *In re Nat'l Sec. Agency Telecomm. Records Litig.*, No. 06-1791 at 1. “These cases, together with a subpoena enforcement action brought by the same Missouri officials who are defendants in the United States’ injunction case concerning that state, were transferred to [Judge Walker] by the Judicial Panel on Multidistrict Litigation (JPML) on February 15, 2007 . . .” *In re Nat'l Sec. Agency Telecomm. Records Litig.*, 630 F. Supp. 2d 1092, 1093–94 (N.D. Cal. 2009) (footnote omitted) (dismissing cases under Section 803 of FISAAA, 50 U.S.C. § 1885b). In addition, one case against the government was litigated separately from the cases in the consolidated MDL, resulting ultimately in a dismissal for lack of standing. *Am. Civil Liberties Union v. Nat'l Sec. Agency*, 493 F.3d 644 (6th Cir. 2007), *cert. denied* 552 U.S. 1179 (2008).

³⁰ “Al-Haramain is a Muslim charity which is active in more than 50 countries. Its activities include building mosques and maintaining various development and education programs. The United Nations Security Council has identified Al-Haramain as an entity belonging to or

The complaint alleged: (1) that the NSA conducted warrantless electronic surveillance of communications between a director or directors of Al-Haramain and the two attorney plaintiffs; (2) that the NSA turned over logs from this surveillance to the Office of Foreign Assets Control (OFAC); and (3) that OFAC then consequently froze Al-Haramain's assets.³² It alleged "violations of FISA, the First, Fourth, and Sixth Amendments to the United States Constitution, the doctrine of separation of powers, and the International Covenant on Civil and Political Rights."³³

Filed under seal with the complaint was a copy of a classified document (the "Sealed Document") that OFAC had inadvertently disclosed to counsel for Al-Haramain as part of a production of unclassified documents relating to Al-Haramain's potential status as a "specially designated global terrorist."³⁴ The Sealed Document apparently provided evidence that the NSA had, in fact, conducted the alleged electronic surveillance, thus establishing the Al-Haramain plaintiffs' standing.³⁵

The problem was that the Government, in addition to asserting that the very subject matter of the case was a state secret, also asserted SSP over

associated with Al Qaeda." *Al-Haramain Islamic Found. v. Bush*, 507 F.3d 1190, 1194 (9th Cir. 2007).

³¹ *Al-Haramain Islamic Found. v. Bush*, 451 F. Supp. 2d 1215 (D. Or. 2006), *rev'd*, 507 F.3d 1190 (9th Cir. 2007). The case was later transferred to Judge Walker by the Judicial Panel on Multidistrict Litigation.

³² *Al-Haramain Islamic Found.*, 451 F. Supp. 2d at 1218.

³³ *Al-Haramain Islamic Found.*, 507 F.3d at 1195.

³⁴ The District Court explained:

[The Office of Foreign Assets Control] inadvertently disclosed this document to counsel for Al-Haramain in late August 2004 as part of a production of unclassified documents relating to Al-Haramain's potential status as a specially designated global terrorist. Lynne Bernabei, an attorney for Al-Haramain . . . , copied and disseminated the materials, including the pertinent document which was labeled "TOP SECRET," to Al-Haramain's directors and Bernabei's co-counsel. In August or September, a reporter from the Washington Post reviewed these documents for an article he was researching. . . . At the request of the FBI, Bernabei and her co-counsel returned their copies of the sensitive document to the FBI. The FBI did not pursue Al-Haramain's directors, whom the government describes as "likely recipients" of the document, to ask them to return their copies.

Al-Haramain Islamic Found., 451 F. Supp. 2d at 1218-19. See also Ryan Singel, *NSA Snooped on Lawyers Knowing Spying Was Illegal, Suit Charges*, WIRED, July 10, 2007, http://www.wired.com/politics/law/news/2007/07/haramain_appeal.

³⁵ According to plaintiffs' attorneys, the Sealed Document "establishes that the government had intercepted attorney-client telephone conversations . . . between an Al-Haramain director in Saudi Arabia and two of the charity's attorneys in Washington, D.C." Thomas H. Nelson & Mark J. Fucile, *When the Government Is Listening in: Advising Clients Under Surveillance*, OR. ST. B. BULL., at 33 (Apr. 2008), available at <http://www.osbar.org/publications/bulletin/08apr/g-men.html>.

the Sealed Document.³⁶ Recall that the SSP has been found by lower courts to justify threshold dismissal of a case in three circumstances: (1) when the “very subject matter” of the case is itself a state secret; (2) when SSP prevents plaintiffs from making a *prima facie* case; or (3) when SSP prevents defendants from asserting a valid defense.³⁷ Thus, if the Sealed Document, which appeared essential to plaintiffs’ Article III standing, and thus to their *prima facie* case, were protected by SSP, Al-Haramain’s claims would still be subject to threshold dismissal.

Al-Haramain countered that Congress had preempted the state secrets privilege, since “FISA vests the courts with control over materials relating to electronic surveillance, subject to ‘appropriate security procedures and protective orders’ [This control] renders the state secrets privilege superfluous in FISA litigation.”³⁸

While skeptical of the Government’s position, the Oregon district court declined to decide the FISA preemption issue³⁹ but found that the very subject matter of the case was not a state secret and denied the Executive’s motion to dismiss, holding that “plaintiffs should have an opportunity to establish standing and make a *prima facie* case, even if they must do so *in camera*.”⁴⁰ The Government had, in fact, conceded that “Plaintiffs remain free to make any allegations and assert any arguments in support of their standing, or any other argument, as they deem appropriate, and the Court has the power to review the sealed classified document in order to assess Plaintiffs’ claims and arguments.”⁴¹

On interlocutory appeal, the Ninth Circuit agreed that the very subject matter of the case was not a state secret because of the extensive public knowledge about the NSA surveillance program⁴² and affirmed the district

³⁶ See *Al-Haramain Islamic Found.*, 451 F. Supp. 2d at 1229.

³⁷ See *supra* text accompanying notes 11, 12, 14.

³⁸ *Al-Haramain Islamic Found.*, 451 F. Supp. 2d at 1229 (quoting 50 U.S.C. § 1806(f) (2006)).

³⁹ *Al-Haramain Islamic Found.*, 451 F. Supp. 2d at 1231 (“I decline to reach this very difficult question at this time, which involves whether Congress preempted what the government asserts is a constitutionally-based privilege,” but noting that “[t]o accept the government’s argument that Section 1806(f) is only applicable when the government intends to use information against a party would nullify FISA’s private remedy and would be contrary to the plain language of Section 1806(f).”).

⁴⁰ *Id.* at 1226 (describing procedure by which plaintiffs could submit sealed affidavits attesting to the contents of the document from their memories).

⁴¹ *Id.* at 1226–27 (citation omitted).

⁴² *Al-Haramain Islamic Found. v. Bush*, 507 F.3d 1190, 1199 (9th Cir. 2007) (describing how “the American public” has “a wealth of information” about the surveillance program).

We agree with the district court’s conclusion that the very subject matter of the litigation—the government’s alleged warrantless surveillance program under the TSP—is not protected by the state secrets privilege. Two discrete sets of unclassi-

court's denial of dismissal on that basis.⁴³ However, the Ninth Circuit also found after *in camera* review that the Sealed Document was protected by the state secrets privilege and rejected the Oregon district court's "compromise solution."⁴⁴

Without the Sealed Document, the Ninth Circuit held that "Al-Haramain cannot establish that it has standing, and its claims must be dismissed, unless FISA preempts the state secrets privilege."⁴⁵ The court declined to decide the preemption question and instead remanded the case to the district court to consider that question "and for any proceedings collateral to that determination."⁴⁶

IV. PREEMPTION AND ITS INTERACTION WITH SSP

This article has thus far discussed the SSP's operation as an extraordinary common-law evidentiary privilege that can justify threshold dismissal. Congress, however, "retains the ultimate authority to modify or set aside any judicially created rules of evidence and procedure that are not required by the Constitution"⁴⁷ and "has plenary authority over the promul-

fied facts support this determination. First, President Bush and others in the administration publicly acknowledged that in the months following the September 11, 2001, terrorist attacks, the President authorized a communications surveillance program that intercepted the communications of persons with suspected links to Al Qaeda and related terrorist organizations. Second, in 2004, Al-Haramain was officially declared by the government to be a "Specially Designated Global Terrorist" due to its purported ties to Al Qaeda. The subject matter of the litigation—the TSP and the government's warrantless surveillance of persons or entities who, like Al-Haramain, were suspected by the NSA to have connections to terrorists—is simply not a state secret.

Id. at 1197–98.

⁴³ *Id.* at 1201.

⁴⁴ *Id.* at 1203–04; *id.* at 1204–05 ("The Sealed Document, its contents, and any individuals' memories of its contents, even well-reasoned speculation as to its contents, are completely barred from further disclosure in this litigation by the common law state secrets privilege.").

⁴⁵ *Id.* at 1205.

⁴⁶ *Id.* at 1206.

⁴⁷ *Dickerson v. United States*, 530 U.S. 428, 437 (2000).

gation of evidentiary rules for the federal courts.”⁴⁸ It follows that Congress can “preempt” or modify the operation of the SSP by statute.⁴⁹

An early case found that Congress had done so in the Invention Secrecy Act of 1951.⁵⁰ That Act required nondisclosure of otherwise patentable inventions when their disclosure could compromise national security, but because nondisclosure precludes the inventor from receiving or exploiting the patent, it also provided for compensation for inventors through the filing of an administrative claim.⁵¹ After being denied compensation,⁵² the plaintiff brought suit in district court. The government argued that the Act conferred no right to bring suit during the pendency of the secrecy order.⁵³ In the alternative, it argued that its assertion of the state secrets privilege compelled dismissal of the claim.⁵⁴

The court held that the plain language of the statute permitted a claim contesting the administrative finding even while the secrecy order was pending.⁵⁵ The court’s key point was that when Congress creates private rights of action, it subordinates SSP to the requirements of litigation. The court reasoned:

Congress has created rights which it has authorized federal courts to try. Inevitably, by their very nature, the trial of cases involving patent application placed under a secrecy order will always involve matters within the scope of this privilege. Unless Congress has created rights which are completely illusory, existing only at the mercy of government officials, the act must be viewed as waiving the privilege.⁵⁶

⁴⁸ *Usery v. Turner Elkhorn Mining Co.*, 428 U.S. 1, 31 (1976); *see also* *Hawkins v. United States*, 358 U.S. 74, 78 (1958); *Tot v. United States*, 319 U.S. 463, 467 (1943). Congress’s power is limited in one important way: “Although evidentiary matters are governed by the rules, they cannot modify litigants’ substantive rights as to either constitutional or statutory matters.” *In re Sealed Case*, 494 F.3d 139, 143 (D.C. Cir. 2007) (“the rules of evidence must yield when they offend the constitutional trial rights of litigants”) (citations omitted).

⁴⁹ *Reynolds* disclaimed that the state secrets privilege is actually rooted in the Constitution, stating instead that the privilege was “well established in the law of evidence” before Congress had even approved the Federal Rules of Evidence. *United States v. Reynolds*, 345 U.S. 1, 6–7 (1953). Thus, the *Reynolds* Court merely interpreted and applied federal common law. *See id.* at 6 n.9.

⁵⁰ *Halpern v. United States*, 258 F.2d 36 (2d Cir. 1958).

⁵¹ *See id.* at 37.

⁵² *Id.*

⁵³ *Id.* at 38.

⁵⁴ *Id.*

⁵⁵ *Id.* at 44.

⁵⁶ *Id.* at 43 (recognizing that the need to balance the Act’s dual objectives of protecting national security secrets and permitting compensation via a private right of action were adequately served by *ex parte in camera* review of the secret information).

As Al-Haramain argued, it is clear that Congress had preempted the state secrets privilege when it regulated government interception of communications. First, Congress had clearly asserted its power in this area.⁵⁷ As part of FISA, Congress commanded that the procedures of FISA and Title III be the “*exclusive means* by which electronic surveillance . . . and the interception of domestic . . . communications may be conducted.”⁵⁸ Congress gave these requirements teeth by authorizing private persons aggrieved by illegal electronic surveillance to bring lawsuits.⁵⁹

Congress did even more by explicitly providing a procedure when litigation implicates national security. Under section 1806(f) of FISA, in federal cases where “aggrieved persons” seek to discover materials relating to, or information derived from, electronic surveillance, the Attorney General may file “an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States.”⁶⁰ In that event, the court “shall” conduct an *in camera*, *ex parte* review of such materials relating to the surveillance “as may be necessary to determine whether the surveillance . . . was lawfully authorized and conducted.”⁶¹

Section 1806(f) thus reflected two clear Congressional judgments. Congress dictated a protocol whenever a claim of state secrets privilege arises in the context of litigation over electronic surveillance—a process crafted to afford an aggrieved person the chance to make his or her case while still protecting the Government’s legitimate claims of national security.⁶² The legislative history showed that Congress intended for disclosure unless the Government asserted a national security interest. Where “no such assertion is made [in an Attorney General’s affidavit], the Committee envisions that mandatory disclosure of the application and order, and discretio-

⁵⁷ *In re Nat’l Sec. Agency Telecomm. Records Litig.*, 564 F. Supp. 2d 1109, 1116 (N.D. Cal. 2008) (“Congress intended to displace entirely the various warrantless wiretapping and surveillance programs undertaken by the executive branch and to leave no room for the president to undertake warrantless surveillance in the domestic sphere in the future.”).

⁵⁸ *Id.* at 1116 (emphasis added) (quoting 18 U.S.C. § 2511(2)(f) (2006)).

⁵⁹ *See* 18 U.S.C. § 2520(a) (civil cause of action for interception of communications in violation of the Wiretap Act); 50 U.S.C. § 1810 (same for electronic surveillance in violation of FISA); *see also* 18 U.S.C. § 2707(a) (same for unlawful disclosures by communications providers under the Stored Communications Act); 47 U.S.C. § 605(e)(3)(A) (same for unlawful disclosures by communications providers under the Communications Act).

⁶⁰ 50 U.S.C. § 1806(f).

⁶¹ *Id.*

⁶² “Congress . . . anticipated that issues regarding the legality of FISA-authorized surveillance would arise in civil proceedings and . . . it empowered federal district courts to resolve those issues, *ex parte* and *in camera* whenever the Attorney General files an appropriate affidavit under § 1806(f).” *Am. Civil Liberties Union v. Barr*, 952 F.2d 457, 470 (D.C. Cir. 1991).

nary disclosure of other surveillance materials, would be available to the [aggrieved party].”⁶³

Moreover, Congress determined that there could be circumstances in which “the court may disclose to the aggrieved person” information that the Government maintains “would harm the national security . . . under appropriate security procedures.”⁶⁴ Indeed, when FISA was enacted, the legislative history expressly stated:

The conferees agree that an *in camera* and *ex parte* proceeding is appropriate for determining the lawfulness of electronic surveillance in both criminal and civil cases. The conferees also agree that the standard for disclosure in the Senate bill adequately protects the rights of the aggrieved person, and that the provision for security measures and protective orders ensures adequate protection of national security interests.⁶⁵

Unsurprisingly, the district court held that FISA indeed preempts the state secret privilege in cases within FISA’s reach,⁶⁶ finding that, (1) “Congress through FISA established a comprehensive, detailed program to regulate foreign intelligence surveillance in the domestic context;”⁶⁷ (2) Congressional intent to replace the common law privilege can be inferred from FISA’s legislative history,⁶⁸ and (3) section 1806(f) is “in effect a codification of the state secrets privilege for purposes of relevant cases under FISA, as modified to reflect Congress’s precise directive to the federal courts for the handling of materials and information with purported national security implications.”⁶⁹

The district court also made short shrift of the Government’s argument that the constitutional aspects of the SSP prevented Congress from preempting the state secrets privilege, finding that “the authority to protect national security information is neither exclusive nor absolute in the execu-

⁶³ S. REP. NO. 95-701, at 63 (1978); *accord* S. REP. NO. 95-604, pt. I, at 57 (1977).

⁶⁴ 50 U.S.C. § 1806(f).

⁶⁵ Foreign Intelligence Surveillance Act of 1978, H.R. CONF. REP. NO. 95-1720, at 32 (Oct. 5, 1978), *reprinted in* 1978 U.S.C.C.A.N. 4048, 4061; *see also* S. REP. NO. 95-701, at 64 (Mar. 14, 1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4032–33 (calling section 1806(f) “a reasonable balance between an entirely *in camera* proceeding . . . and mandatory disclosure, which might occasionally result in the wholesale revelation of sensitive foreign intelligence information.”).

⁶⁶ *In re Nat’l Sec. Agency Telecomm. Records Litig.*, 564 F. Supp. 2d 1109, 1115–24 (N.D. Ca. 2008) (using the preemption framework of *Illinois v. Milwaukee*, 406 U.S. 91, 107 n.9 (1972), under which federal common law applies “[u]ntil the field has been made the subject of comprehensive legislation.”).

⁶⁷ *In re Nat’l Sec. Agency Telecomm. Records Litig.*, 564 F. Supp. 2d at 1118.

⁶⁸ *See id.* at 1120.

⁶⁹ *Id.* at 1119.

tive branch,” and that “[w]hen Congress acts to contravene the president’s authority, federal courts must give effect to what Congress has required.”⁷⁰

V. THE STRUGGLE AFTER PREEMPTION

As the district court noted, however, “[t]he determination that FISA preempts the state secrets privilege does not necessarily clear the way for plaintiffs.”⁷¹ The first problem was that only an “aggrieved person” may claim damages under FISA⁷² or invoke the discovery provision.⁷³ Defendants argued that the court could not decide whether the plaintiffs were “aggrieved persons” given the Government’s successful state secrets privilege assertion as to the Sealed Document,⁷⁴ and that even “assuming *arguendo* that FISA ‘preempts’ the state secrets privilege . . . plaintiffs would still be unable to establish their standing . . . without ‘inherently risk[ing] or requir[ing] the disclosure of state secrets to the plaintiffs and the public at large.’”⁷⁵

The district court agreed that the plaintiffs could not use the Sealed Document to establish “aggrieved person” status but permitted the plaintiffs to amend their complaint:

Plaintiffs must first establish “aggrieved person” status without the use of the Sealed Document and may then bring a “motion or request” under § 1806(f) in response to which the attorney general may file an affidavit opposing disclosure. At that point, in camera review of materials responsive to the motion or request, including the Sealed Document, might well be appropriate. . . . [P]laintiffs must present to the court enough specifics based on non-classified evidence to establish their “aggrieved person” status under FISA.⁷⁶

In its next *Al-Haramain* decision (the January 5 Order), the district court found that plaintiffs had established that they were “aggrieved per-

⁷⁰ *Id.* at 1121 (noting that “*unless Congress specifically has provided otherwise*, courts traditionally have been reluctant to intrude upon the authority of the Executive in military and national security affairs.” (emphasis in district court opinion)), quoting *Dep’t of the Navy v. Egan*, 484 U.S. 518, 527 (1988).

⁷¹ *In re Nat’l Sec. Agency Telecomm. Records Litig.*, 564 F. Supp. 2d at 1125.

⁷² 50 U.S.C. § 1810 (2006).

⁷³ *Id.* § 1806(f).

⁷⁴ *In re Nat’l Sec. Agency Telecomm. Records Litig.*, 564 F. Supp. 2d at 1124.

⁷⁵ *Id.* at 1132 (alterations in district court opinion) (citation omitted). Indeed, the Government had even argued that the district court could not adjudicate plaintiffs’ standing or the merits. See *infra* text accompanying note 109. The Government does not dispute the use of section 1806(f) in cases where the Government has affirmatively acknowledged the fact of FISA surveillance. See, e.g., *Al-Kidd v. Gonzales*, No. CV 05-093-EJL (MHW), 2008 WL 5123009 (D. Idaho Dec. 4, 2008).

⁷⁶ *In re Nat’l Sec. Agency Telecomm. Records Litig.*, 564 F. Supp. 2d at 1135.

sons,” denying the Executive’s third motion to dismiss⁷⁷ and granting plaintiffs’ motion for discovery pursuant to FISA § 1806(f).⁷⁸

The January 5 Order addressed:

[T]he logistical problems and process concerns that attend considering classified evidence and issuing rulings based thereon. Measures necessary to limit the disclosure of classified or other secret evidence must in some manner restrict the participation of parties who do not control the secret evidence and of the press and the public at large. The court’s next steps will prioritize two interests: protecting classified evidence from disclosure and enabling plaintiffs to prosecute their action.⁷⁹

The district court was clear that that its case management approach aimed not only at carrying out Congressional will under FISA, but also at ensuring plaintiffs’ due process rights.

Unless counsel for plaintiffs are granted access to the court’s rulings and, possibly, to at least some of defendants’ classified filings, however, the entire remaining course of this litigation will be *ex parte*. This outcome would deprive plaintiffs of due process to an extent inconsistent with Congress’s purpose in enacting FISA’s sections 1806(f) and 1810.⁸⁰

Accordingly, the January 5 Order provided for plaintiffs’ counsel to obtain top secret and sensitive compartmented information security clearances and ordered the government to review its classified submissions in this case and determine whether any could be declassified.⁸¹

⁷⁷ *In re Nat’l Sec. Agency Telecomm. Records Litig.*, 595 F. Supp. 2d 1077, 1083 (N.D. Cal. 2009). This case notes that:

Defendants’ position boils down to this: only affirmative confirmation by the government or equally probative evidence will meet the “aggrieved person” test; the government is not required to confirm surveillance and the information is not otherwise available without invading the SSP. In defendants’ view, therefore, plaintiffs simply cannot proceed on their claim without the government’s active cooperation—and the government has evinced no intention of cooperating here.

Id.

⁷⁸ *Id.* at 1089.

⁷⁹ *Id.*

⁸⁰ *Id.* The district court later stated:

I have no intention of reviewing the sealed document [containing classified information] until we get all of these pieces in place so that we can proceed in a judicial fashion; and by that I mean a fashion in which both parties have access to the material upon which the court makes a decision.

In re Nat’l Sec. Agency Telecomm. Records Litig., No. 06-1791 (VRW), 2009 WL 1468792, at *1 (N.D. Cal. May 22, 2009) (quoting Jan. 23, 2009 case management transcript).

⁸¹ *In re Nat’l Sec. Agency Telecomm. Records Litig.*, 595 F. Supp. 2d at 1089–90.

VI. THE EXECUTIVE RESISTS

The January 5 Order marked the beginning of intense resistance by the Government. Seemingly at the heart of the resistance was the Executive's refusal to permit litigant access to classified information. First, the Executive quickly filed a notice of appeal with the Ninth Circuit and moved for a stay in district court pending appeal and certification of interlocutory appeal.⁸²

Critical here was the Government's position that the court had no authority to order disclosure to Al-Haramain's counsel:

[U]nder applicable Executive Orders, even if a person is found to be "suitable" to receive access to classified information after an investigation of their background and, thus, is granted a "security clearance," the agency that originates the information at issue must make a separate "need-to-know" determination that actually grants access to classified information.⁸³

That is, the agency must determine that the person has a "demonstrated 'need to know' classified information in connection with the performance of a 'governmental function' that is 'lawful and authorized' by the agency."⁸⁴ Perhaps unsurprisingly, the director of the NSA had determined:

[T]hat neither plaintiffs nor their counsel have a need for access to classified NSA information that has been (or would be) excluded under the state secrets privilege assertion. . . . [I]t does not serve a governmental function . . . to disclose the classified NSA information . . . simply to assist the plaintiffs' counsel in representing the interests of private parties who have filed suit against the NSA and who seek to obtain disclosure of information related to NSA intelligence sources and methods.⁸⁵

Indeed, the Government's reply complained that the January 5 Order "operates to take that determination from the Government in proceedings under Section 1806(f)" and "presents a clear-cut conflict between the Court and the Executive Branch over whether plaintiffs may receive classified information."⁸⁶

⁸² See *In re Nat'l Sec. Agency Telecomm. Records Litig.*, 2009 WL 1468792, at *1 (describing procedural history).

⁸³ Defendants' Notice of Motion and Motion for a Stay Pending Appeal and for Certification of an Interlocutory Appeal at 12, *Al-Haramain Islamic Found. v. Bush*, No. 07-CV-109 (VRW) (N.D. Cal. Jan. 19, 2009) (citations omitted), available at <http://www.eff.org/files/filenode/att/alharamainstaymotion11909.pdf>.

⁸⁴ *Id.* at 13.

⁸⁵ *Id.* at 13 (citations omitted).

⁸⁶ Government Defendants' Reply in Support of Motion to Stay Proceedings Pending Appeal and Certification of Interlocutory Appeal Under 28 U.S.C. § 1292(b) at 11, *Al-*

The district court denied the motion and ordered defendants to inform the court by February 27 how they intended to comply with the January 5 Order, including provisions for litigant access.⁸⁷ By this time, the Justice Department had determined that two of plaintiffs' counsel were eligible for access to classified information.⁸⁸

The district court also issued a third order requiring the Government to respond to questions about "the Court's authority to decide whether plaintiffs' counsel have a 'need to know' some or all of the classified information filed with the Court in this case."⁸⁹ Undeterred, the Government continued to insist that plaintiffs and their counsel lacked "need to know"⁹⁰ and made an emergency motion to the Ninth Circuit for a stay pending appeal of the January 5 Order, which was swiftly rejected for lack of jurisdiction.⁹¹

The very day that the Ninth Circuit closed off the interlocutory appeal, the Executive began its second phase of resistance by refusing to engage with plaintiffs on the substance of the January 5 Order. The Executive

Haramain Islamic Found. v. Obama, No. 09-CV-01791 (VRW) (N.D. Cal. Feb. 11, 2009), available at <http://www.jdsupra.com/post/documentViewer.aspx?fid=bc04e35b-ac56-4d83-aa27-c58e3d11556c>.

⁸⁷ Order at 3, Al-Haramain Islamic Found. v. Bush, No. 06-1791 (VRW) (N.D. Cal. Feb. 13, 2009), available at <http://www.eff.org/files/filenode/att/alharamainorder21309.pdf>.

⁸⁸ Plaintiffs' Supplemental Case Management Statement at 1, Al-Haramain Islamic Found. v. Bush, No. 06-CV-1791 (VRW) (N.D. Cal. Feb. 18, 2009), available at <http://www.eff.org/files/filenode/att/alharamaincms21809.pdf> ("On February 12, 2009, the Department of Justice Litigation Security Section advised plaintiffs' counsel that background investigations for plaintiffs' counsel Jon B. Eisenberg and Steven Goldberg have been 'favorably adjudicated' within the meaning of Executive Order No. 12968, § 3.1(b) (1995)."); see also Government Defendants' Response to Court Orders Concerning Compliance with the January 5 Order [Dkt. 71] and Response to Plaintiffs' Supplemental Case Management Report [Dkt. 75] at 4, Al-Haramain Islamic Found. v. Obama, No. 07-CV-00109 (VRW) (N.D. Cal. Feb. 27, 2009) [hereinafter Government Defendants' Response to Court Orders and Response to Plaintiffs' Supplemental Case Management Report], available at <http://www.eff.org/files/filenode/att/govtresponsealhara22709.pdf> ("[T]wo of plaintiffs' counsel are eligible for access to classified information.").

⁸⁹ Order, Al-Haramain Islamic Found. v. Bush, No. 06-CV-01791 (VRW) (N.D. Cal. Feb. 19, 2009) (internal quotation marks omitted), available at <http://www.eff.org/files/filenode/att/orderstay21909.pdf>.

⁹⁰ Emergency Motion for Stay Pending Appeal at 1, Al-Haramain Islamic Found. v. Obama, No. 09-15266 (9th Cir. Feb. 20, 2009), available at <http://www.eff.org/files/GovtEmergStay9thCir.pdf> ("[P]laintiffs do not have the requisite 'need to know' the information . . .").

⁹¹ Order, Al-Haramain Islamic Found. v. Obama, No. 09-15266 (9th Cir. Feb. 27, 2009), available at http://www.wired.com/images_blogs/threatlevel/files/9thcirc.pdf ("We agree with the district court that the January 5, 2009 order is not appropriate for interlocutory appeal. The government's appeal is DISMISSED for lack of jurisdiction. The government's motion for a stay is DENIED as moot.").

maintained that plaintiffs' counsel could not be given access to classified information.

In this case, the relevant official . . . has determined that counsel *do not* have a need to know. This decision is committed to the discretion of the Executive Branch, and is not subject to judicial review. Moreover, the Court does not have independent power, either under its supervisory authority, or under authority analogous to that granted by the Classified Information Procedures Act ("CIPA"), 18 U.S.C. App. 3, to order the Government to grant counsel access to classified information when the Executive Branch has denied them such access. Therefore, the Government respectfully suggests that the Court should not take further steps at this time that would result in plaintiffs' counsel being granted access to the classified information at issue.⁹²

The district court was less than pleased with the Executive's response and ordered the parties:

[T]o meet and confer regarding the entry of an appropriate protective order which shall be entered herein before the court rules on the merits. . . . The parties shall submit to the court a stipulated protective order on or before May 8, 2009. If the parties are unable to agree on all terms, they shall jointly submit a document containing all agreed terms together with a document setting forth the terms about which they are unable to reach agreement and the respective positions of the parties with regard to each such term. The court will then consider the submissions and enter a protective order under which this case may resume forward progress.⁹³

When the Government refused to stipulate to a protective order,⁹⁴ the district court ordered the Government to show cause:

[W]hy, as a sanction for failing to obey the court's orders:

- (1) defendants should not be prohibited, under FRCP 37(b)(2)(ii), from opposing the liability component of plaintiffs' claim under 50 USC § 181 —that is, from denying that plaintiffs are "aggrieved persons" who were subjected to electronic surveillance; and

⁹² Government Defendants' Response to Court Orders and Response to Plaintiffs' Supplemental Case Management Report, *supra* note 88, at 2 (emphasis in original).

⁹³ Order at 2–3, *Al-Haramain Islamic Found. v. Bush*, No. 06-CV-01791 (VRW) (N.D. Cal. Apr. 17, 2009) [hereinafter April 17, 2009 Order], available at <http://www.eff.org/files/filenode/att/alharamainprotectiveorder41709.pdf>.

⁹⁴ Joint Submission in Response to Court's April 17, 2009 Order [Dkt. 84] at 32, *Al-Haramain Islamic Found. v. Obama*, No. 06-CV-01791 (VRW) (N.D. Cal. May 15, 2009) [hereinafter Joint Submission in Response to Court's April 17, 2009 Order], available at <http://www.eff.org/files/filenode/att/jointresponsealharamain51509.pdf>.

(2) the court should not deem liability under 50 USC § 1810 established and proceed to determine the amount of damages to be awarded to plaintiffs.⁹⁵

Eventually, the district court dodged the looming constitutional issue. It instead ordered:

Plaintiffs shall base their motion on non-classified evidence. If defendants rely upon the Sealed Document or other classified evidence in response, the court will enter a protective order and produce such classified evidence to those of plaintiffs' counsel who have obtained top secret/sensitive compartmented information clearances . . . for their review. Otherwise, the court will consider the motion on non-classified evidence.⁹⁶

The briefing occurred without classified evidence, although in one last gasp, the Executive sought to end-run the district court and, on November 9, lodged a classified declaration from the Director of the Office of National Intelligence with the Ninth Circuit. This too was rejected.⁹⁷ *Al-Haramain* is under submission in the district court as of this writing.

VII. DISCUSSION

Ostensibly, the Government's recalcitrance was about the district court's plan for plaintiffs' counsel to obtain security clearances in order to enable their potential access to classified information. Yet that recalcitrance is puzzling on its face. First, the Government's position rested mainly on non-statutory, Executive Branch rules about classified information, completely ignoring the fact that the dispute was about access within a judicial, litigation context.⁹⁸ Its argument that the court lacks "independent power,

⁹⁵ *In re Nat'l Sec. Agency Telecomm. Records Litig.*, No. 06-1791 (VRW), 2009 WL 1468792, at *2 (N.D. Cal. May 22, 2009) (pertaining to *Al-Haramain Islamic Found. v. Bush*).

⁹⁶ Order at 1–2, *Al-Haramain Islamic Found. v. Obama*, No. 06-CV-01791 (VRW) (N.D. Cal. June 5, 2009), available at <http://www.eff.org/files/filenode/att/briefingorder6509.pdf>.

⁹⁷ Order, *Al-Haramain Islamic Found. v. Bush*, No. 09-36083 (9th Cir. Nov. 23, 2009), available at <http://www.eff.org/files/filenode/att/alharamainnotice112309.pdf> ("Appellees *Al-Haramain Islamic Foundation, Inc.*, Wendell Belew, and Asim Ghafoor's Motion to Strike appellants' lodging of an *In Camera, Ex Parte* declaration of the Director of National Intelligence is GRANTED. This court does not have jurisdiction over the case as the mandate was issued on January 16, 2008.").

⁹⁸ Similar issues were raised by a lawsuit brought by former Drug Enforcement Administration employee Richard Horn alleging that a former State Department employee and a former CIA operative illegally bugged Horn's home in Burma in the early 1990s. Although the district court initially upheld the Government's assertion of the state secret privilege over the CIA operative's identity and dismissed the case, the D.C. Circuit reversed the dismissal and permitted Horn to proceed. *In re Sealed Case*, 494 F.3d 139, 154 (D.C. Cir. 2007). On remand, the district court learned that the CIA operative's identity had been unclassified

either under its supervisory authority, or under authority analogous to that granted by the Classified Information Procedures Act . . . to order the Government to grant counsel access to classified information when the Executive Branch has denied them such access”⁹⁹ is especially ironic with respect to the Sealed Document, which not only had already been disclosed to Al-Haramain and his counsel, but had entered the judicial record.¹⁰⁰

Moreover, FISA expressly authorizes the district court to “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.”¹⁰¹ While there is an obvious question as to when such disclosure is “necessary,” Congress clearly expected that the district court would make that determination.¹⁰² Thus, in *Al-Haramain* all three branches plainly have roles to play, and the Executive had already played its national security role by determining that Al-Haramain’s counsel were eligible for access to classified information at the top secret and sensitive compartmented information security clearance level.

Second, the January 5 Order was not itself about any such disclosures, but rather aimed mainly to begin the process by which any such disclosures could be made if “necessary”—not to decide whether any disclo-

since 2002, after which the court found that the state secrets privilege no longer applied, and ordered the use of CIPA-like procedures to manage the classified information in the case. *Horn v. Huddle*, 636 F. Supp. 2d 10, 18–19 (D.D.C. 2009). Over the Government’s objections, the district court then found that the parties’ counsel had a “need to know” entitling them to have access to the classified information that their clients already possessed. *Horn v. Huddle*, 647 F. Supp. 2d 55, 65 n.18, 66 (D.D.C. 2009).

[I]t is the Court’s determination that the attorneys need to be involved . . . for the case to move forward while minimizing the risk to national security. The deference generally granted the Executive Branch in matters of classification and national security must yield when the Executive attempts to exert control over the courtroom.

Id. at 65–66 (footnote omitted). The district court noted, for instance, that the plaintiff’s attorneys had previously been granted security clearances and were able to see classified information, but once the clearances lapsed the Government asserted that they no longer had “need to know.” *Id.* at 63 n.11. The Government eventually settled with Horn for \$3 million. Settlement Agreement at 2, *Horn v. Huddle*, No. 1:94-CV-1756 (RCL) (D.D.C. Nov. 3, 2009), available at http://www.wired.com/images_blogs/threatlevel/2009/11/horn-v-huddle-settlement.pdf.

⁹⁹ Government Defendants’ Response to Court Orders and Response to Plaintiffs’ Supplemental Case Management Report, *supra* note 88, at 2.

¹⁰⁰ Even ignoring the unusual circumstances surrounding the Sealed Document, the Government well knew that courts of appeal had permitted the use of CIPA-like procedures in a civil case. In *Horn v. Huddle*, the court of appeals had held in 2007 that CIPA-like procedures were permissible. *In re Sealed Case*, 494 F.3d at 154.

¹⁰¹ 50 U.S.C. § 1806(f) (2006).

¹⁰² See *supra* text accompanying note 65.

sure would be “necessary.” The district court made clear that its initial step would be to “review the Sealed Document *ex parte* and *in camera*” and “then issue an order regarding whether plaintiffs may proceed—that is, whether the Sealed Document establishes that plaintiffs were subject to electronic surveillance not authorized by FISA.”¹⁰³

Perhaps the Government’s recalcitrance was rooted in its continuing refusal to accept the district court’s ruling that FISA indeed preempted the state secrets privilege.¹⁰⁴ In its May 15 submission to the district court, it reiterated that position by stating:

The Government recognizes that this Court disagrees with its position and has held that FISA Section 1806 preempts the state secrets privilege and provides authority for the disclosure of classified information in this case. But the Government respectfully maintains its position, explained at length in previous filings, that the Court’s prior rulings are in error and should be reviewed before any disclosures occur that would actually negate that privilege assertion.¹⁰⁵

Even this desire for appellate review makes little sense. As already explained, nothing in the January 5 Order or any of the later orders would actually have disclosed anything that would negate the Government’s privilege claim. In addition, if the district court did order disclosure to plaintiffs or their counsel, such an order is statutorily deemed “final” and subject to appellate review.¹⁰⁶

In any case, if the Government’s litigation tactics were aimed at getting the Ninth Circuit to review the district court’s earlier preemption ruling prior to any disclosure to the plaintiffs, one would have expected an end to the tactics after the Ninth Circuit declared that it lacked jurisdiction to review the January 5 Order.¹⁰⁷

¹⁰³ *In re Nat’l Sec. Agency Telecomms. Records Litig.*, 595 F. Supp. 2d 1077, 1089 (N.D. Cal 2009).

¹⁰⁴ Government Defendants’ Response to Court Orders and Response to Plaintiffs’ Supplemental Case Management Report, *supra* note 88, at 5.

¹⁰⁵ Joint Submission in Response to Court’s April 17, 2009 Order, *supra* note 94, at 18 (footnote omitted).

¹⁰⁶ *See* 50 U.S.C. § 1806(h).

[D]ecisions under this section that electronic surveillance was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to a surveillance *shall be final orders* and binding upon all courts of the United States and the several States except a United States court of appeals and the Supreme Court.

Id. (emphasis added).

¹⁰⁷ Indeed, the district court had assumed that this desire for appellate review was the Government’s point:

It would seem that the Government's ultimate position is that there can be no judicial review in cases such as *Al-Haramain*, even when Congress has spoken clearly. In its second motion to dismiss in *Al-Haramain*, the Government essentially argued that the courts could adjudicate neither standing nor the merits. Seizing upon the Ninth Circuit's statement that "the Sealed Document is protected by the state secrets privilege, along with the information as to whether the government surveilled Al-Haramain,"¹⁰⁸ the Government argued that:

[A]ny effort to establish whether the plaintiffs are an aggrieved party . . . would inherently risk or require the disclosure of state secrets to the plaintiffs and the public at large, and thus cause the very harm to national security identified by the Court of Appeals. For example . . . the Court would first have to ascertain whether the individual plaintiffs are "aggrieved" parties as defined by the FISA. If none of the plaintiffs are aggrieved parties, the case could not proceed, but such a holding would reveal to plaintiffs and the public at large information that is protected by the state secrets privilege—namely, that certain individuals were not subject to alleged surveillance. Conversely, if the case did proceed, it could do so only as to an aggrieved party, which would confirm that a plaintiff was subject to surveillance.

In addition, assuming there were an aggrieved party in this case, at some point the Court would have to grant or deny relief. If an aggrieved plaintiff were to lose on the merits, only that plaintiff could appeal—and that fact would be disclosed or become apparent on the public record even if the substance of the Court's underlying deliberations remained secret. Likewise, if the government were to lose on the merits . . . as to a particular aggrieved plaintiff, that too would either have to be disclosed or would become apparent upon any appeal. Thus, even if every effort were made to protect any underlying information concerning alleged surveillance, serious risks remain that basic facts concerning whether or not there had been any surveillance in this case would be inadvertently revealed in the process.¹⁰⁹

The United States . . . has offered up three similar-sounding alternatives all of which appear geared toward obtaining a stay of this court's proceedings and review by the court of appeals, even though its simultaneous attempts to obtain review as of right and by means of an interlocutory appeal of the January 5 order failed in February. As both this court and the court of appeals have determined that this matter is properly before the court, the United States should now comply with the court's orders.

April 17, 2009 Order, *supra* note 93, at 1–2 (citations omitted).

¹⁰⁸ *Al-Haramain Islamic Found. v. Bush*, 507 F.3d 1190, 1203 (9th Cir. 2007).

¹⁰⁹ Memorandum in Support of Defendants' Second Motion to Dismiss for Summary Judgment at 23–24, *Al-Haramain Islamic Found. v. Bush*, No. 06-CV-01791 (VRW) (N.D.

The breadth of the Government's hubris is as startling as it is specious. After all, the Ninth Circuit clearly held that "Al-Haramain cannot establish that it has standing, and its claims must be dismissed, *unless FISA preempts the state secrets privilege*."¹¹⁰ Conversely, if FISA does preempt the privilege, plaintiffs can establish standing and the courts can adjudicate whether plaintiffs were surveilled. Had the Ninth Circuit believed that such adjudication would harm national security, it would not have remanded the case to the district court for a determination of whether FISA preempts the state secrets privilege and "any proceedings collateral to that determination."¹¹¹

It could hardly be otherwise. Congress provided a civil cause of action for "aggrieved persons" to challenge alleged unlawful electronic surveillance and an *ex parte, in camera* procedure for district court review. *Reynolds* made clear that "a complete abandonment of judicial control would lead to intolerable abuses,"¹¹² and thus "[j]udicial control over the evidence in a case cannot be abdicated to the caprice of executive officers."¹¹³ To accept the Government's assertion that the merits cannot be decided would negate Congressional power by preventing any judicial determination of whether the Executive had acted illegally in an area where all three branches share constitutional responsibility.

More generally, the Government's attempt to use the state secrets privilege and its positional advantage with respect to classified information access in cases such as *Al-Haramain* strikes at both due process and Article III. As we have already seen, the district courts in both *Horn*¹¹⁴ and *Al-Haramain* were acutely concerned about the fundamental fairness of litigation without some level of access to relevant classified information. To expand the impact of the state secrets privilege "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" that "would be manifestly unfair to a plaintiff."¹¹⁵

Nor can courts truly perform their core judicial function without active adversary process because "[a]n informed, independent judiciary presumes an informed, independent bar,"¹¹⁶ and "the ordinary course of litiga-

Cal. Mar. 14, 2008) (footnote omitted), *available at* <http://www.eff.org/files/filenode/att/haramain2ndmotion.pdf>.

¹¹⁰ *Al-Haramain Islamic Found.*, 507 F.3d at 1205 (emphasis added).

¹¹¹ *Id.* at 1206.

¹¹² *United States v. Reynolds*, 345 U.S. 1, 8 (1953).

¹¹³ *Id.* at 9–10.

¹¹⁴ *See supra* note 98.

¹¹⁵ *In re Sealed Case*, 494 F.3d 139, 150 (2007).

¹¹⁶ *Legal Servs. Corp. v. Velazquez*, 531 U.S. 533, 545 (2001).

tion involves the expression of theories and postulates on both, or multiple, sides of an issue.”¹¹⁷ One can reasonably fear for judicial integrity itself.¹¹⁸

VIII. CONCLUSION

This article has mostly been an exercise in description. Its cautionary point is simple: the Executive’s initial control of national security information gives it tremendous litigation advantages, even when Congress has authorized courts to receive national security information precisely in order to enable judicial review. In such situations, ordinary pretrial and discovery practice faces significant Executive resistance over access to information that “aggrieved persons” need to challenge the legality of surveillance and courts need to adjudicate these challenges. As we have seen, the Executive resists even when a judicial order of disclosure to litigants is subject to appeal as a final judgment and when the court attempts to implement necessary litigation management procedures, such as security clearances and protective orders, well in advance of any actual disclosure to litigants.¹¹⁹

It is difficult to imagine how courts could proceed more carefully than the Ninth Circuit and the district courts in *Al-Haramain* did. Congress clearly intended FISA and the section 1806(f) procedures to operate as a mechanism by which courts could manage litigation over the legality of warrantless surveillance. Thus, the first lesson here is probably for Congress: any legislative preemption or reform of the state secrets privilege must anticipate the various procedural hurdles that a highly resistant Executive will use to delay or frustrate litigation.

Perhaps more importantly, Congress cannot itself enforce individual rights, statutory or constitutional; it needs litigants to bring cases, and it needs courts to hear them. Yet the Government’s position on “need to know” essentially asserts that litigation authorized by Congress precisely in

¹¹⁷ *Id.* at 548.

¹¹⁸ The Supreme Court had criticized the scheme in *Velazquez* for creating “doubt whether the truncated representation had resulted in complete analysis of the case, full advice to the client, and proper presentation to the court,” believing “courts and the public would come to question the adequacy and fairness” of the proceedings. *Id.* at 546.

¹¹⁹ Indeed, the resolution of the *Horn* litigation shows how important this issue is to the Government: the settlement agreement expressly provides that Horn agrees “not to oppose any motion to vacate” the district court’s orders regarding CIPA-like procedures and providing for litigant access to classified information. Settlement Agreement, *supra* note 98, at 4.

The United States contends that vacatur is of significant interest to the Government because the Government otherwise would prefer to contest what it sees as an erroneous application of the law. Plaintiff understands that the opportunity to seek vacatur is a significant reason why the Government is entering into settlement.

Id.

order to check unlawful government surveillance is not a “governmental function.” *Al-Haramain* thus presents a vision of sweeping Executive power that ignores Congress and the courts even when they are working together to protect individual rights against Executive abuse.