# NSA Surveillance: The Litigation and its Implications

*By Thomas R. McCarthy**

On December 16, 2005, the *New York Times*[1] reported that President Bush had authorized the National Security Agency (NSA) to conduct surveillance of communications within the United States in the absence of court approval for the purposes of effectuating the mandate of the joint resolution Congress passed shortly after the September 11, 2001 terror attacks.[2] The day after the news leak, President Bush, in his weekly radio address, confirmed the existence of the Terrorist Surveillance Program ("TSP"). The President stated that he had "authorized the National Security Agency, consistent with U.S. law and the Constitution, to intercept the international communications of people with known links to al Qaeda and related terrorist organizations," and he gave a limited description of the process used periodically to review and reauthorize the TSP.[3] An additional element of the TSP was alleged in May 2006, when *USA Today* reported that AT&T, Verizon, and BellSouth had provided the Government with access to the communications records of tens of millions of Americans,[4] a charge the companies have consistently denied.[5] The Government has not confirmed the existence of this alleged "records" element of the TSP.

The revelation of the TSP's existence elicited substantial press attention and resulted in the filing of numerous lawsuits[6] challenging its lawfulness under the Constitution and various federal statutes—including the Foreign Intelligence Surveillance Act (FISA),[7] the Wiretap Act,[8] and the Electronic Communications Privacy Act[9]—as well as under various state constitutions and statutes. Recently, the District Courts for the Northern District of California and the Eastern District of Michigan have issued controversial opinions in two cases currently pending on appeal to the Ninth and Sixth Circuit Courts of Appeals, respectively.[10] The outcome of these appeals has the potential to impact profoundly the separation of powers and alter the balance between the protection of civil liberties and the ability of the Government to protect the nation against future terrorist attacks.

## Notable Litigation

*ACLU v. NSA* was filed in January of 2006 in the Eastern District of Michigan, challenging the lawfulness of the TSP and requesting declaratory and injunctive relief.[11] The Government responded by filing a motion to dismiss or, in the alternative, for summary judgment, relying largely on its assertion of the state secrets privilege.[12] On August 17, 2006, Judge Anna Diggs Taylor issued an opinion granting summary judgment in favor of the Government with respect to the alleged records element of the TSP, while declaring the confirmed "contents" element of the TSP unconstitutional and permanently enjoining the NSA from continuing to conduct it.[13] The NSA appealed to the Sixth Circuit Court of Appeals, which has stayed the district court's order while the appeal is pending.[14]

*Hepting v. AT&T Corp.* challenges the constitutionality of the TSP in the context of a civil claim against AT&T for its alleged cooperation with the NSA's surveillance activities, and was filed in the Northern District of California by the Electronic Frontier Foundation on behalf of AT&T customers.[15] The Judicial Panel on Multidistrict Litigation consolidated several similar actions into a multidistrict litigation ("MDL") with *Hepting* as the lead case.[16] Believing federal interests were at stake, the Department of Justice intervened in the case. As in *ACLU v. NSA*, the Government filed a motion to dismiss the case on the basis of the state secrets privilege, with AT&T claiming additional common law and qualified immunities.[17] The court engaged in in camera and ex parte review of certain classified documents, and on July 20, 2006, Judge Vaughn R. Walker denied these motions. The defendants appealed to the Ninth Circuit Court of Appeals, and Judge Walker is presently considering the defendants' motions to stay proceedings while the appeal is pending.

## Important Constitutional Questions

There are a number of constitutional questions at the heart of the ultimate question of the legality of the TSP. First, the plaintiffs in the suits filed claim that the TSP violates the First Amendment because it chills their overseas communications, "disrupting [their ability] to talk with sources, locate witnesses, conduct scholarship, and engage in advocacy."[18] Although the court in *ACLU v. NSA* found such a chilling effect,[19] it is unclear the asserted fear can be demonstrated to be objectively reasonable given that the Government has refused to divulge any information as to the identity of the intercepted communicants.[20] The Supreme Court has rejected such speculative claims in a case challenging "the Department of the Army's alleged 'surveillance of lawful and peaceful civilian political activity.'"[21] In that case, the Court explained that "[a]llegations of a subjective 'chill' are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm."[22]

Second, plaintiffs argue that the contents element of the TSP violates the Fourth Amendment because it permits the NSA to intercept communications in the absence of either a warrant or probable cause.[23] Although Judge Taylor held that the confirmed contents element of the TSP violates the Fourth Amendment, there are a number of reasons why a warrant might not be required.[24] As a principal matter, it is not clear that the Fourth Amendment even applies in this context. For example, this Amendment does not apply to non-citizens abroad.[25] Nor does it apply to foreign aggressors.[26]

In addition, the Government has argued that no warrant is required because the President has "inherent constitutional authority to conduct warrantless searches for foreign intelligence purposes" pursuant to his authority over foreign affairs and his power as Commander-in-Chief.[27] Indeed, the Foreign Intelligence Surveillance Court of Review has explained that the President has inherent constitutional authority to conduct

** Thomas R. McCarthy is an associate at Wiley Rein and former law clerk to the Honorable David B. Sentelle of the United States Court of Appeals for the D.C. Circuit. He recently co-authored a brief in the United States Court of Appeals for the Sixth Circuit on behalf of several amici supporting the United States in litigation challenging the lawfulness of the NSA Terrorist Surveillance Program.*

foreign intelligence surveillance.[28] Even aside from these arguments, it is possible that the warrant requirement is not applicable because the situation involves "special needs" that go beyond basic law enforcement.[29] Likewise, the warrant requirement may not be applicable because the nature of the intercepted calls—"international communications of people with known links to Al Qaeda and related terrorist organizations"[30]—is such that the callers had a reduced expectation of privacy.[31]

Third, plaintiffs in both cases have argued that, by operating outside the strictures of FISA, the Wiretap Act and ECPA,[32] the TSP constitutes a violation of the separation of powers.[33] Conversely, it can be argued that to the extent that electronic surveillance is a tool of war, any attempt to limit the President's ability to utilize this tool could constitute an unconstitutional encroachment on his powers as Commander-in-Chief under Article II of the Constitution.[34] Or, it could be argued that the courts should find that Congress impliedly authorized the TSP when it enacted the AUMF in order to avoid ruling on this fundamental constitutional question.[35]

Resolution of these issues implicates not only the Government and its efforts in the War on Terror. A number of these cases challenging the TSP include private telecommunications companies as defendants. These private defendants may well be entitled to protection from liability even if the TSP is ultimately found unlawful, to the extent that they cooperated with government investigations under the assumption that the Government's exercise of its authority was lawful.

### A Threshold Question: State Secrets

Perhaps the most important issue presented in these cases, practically speaking, is the threshold issue of state secrets, because it may be dispositive of all of these cases. This privilege protects confidential government information from discovery where revelation would be inimical to national security.[36] It can require dismissal of a case in three distinct ways.[37] First, a successful claim of the privilege removes from consideration evidence that may be necessary for the plaintiff to establish the prima facie elements of his claim. Second, summary judgment may be required if the evidence excluded would otherwise provide the defendant with a valid defense to the claim. Third, if the "very subject matter of the action" is itself a state secret, then the court should dismiss the action in order to respect the separation of powers and protect national security.[38] For example, the Supreme Court has a long history of dismissing cases in which a plaintiff sues the Government over a covert agreement between the two parties.[39]

The federal courts have set out guidelines for courts to consider when faced with a claim of the state secrets privilege.[40] As a general matter, "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, and respecting which it will not allow the confidence to be violated."[41] Thus, where the privilege applies, it is absolute.[42] Moreover, judicial deference to Executive assertions of the privilege is appropriate. That is, "courts must [] bear in mind the Executive Branch's preeminent authority over military and diplomatic matters and its greater expertise relative to the judicial branch in predicting the effect of a particular disclosure on national security."[43] In addition, the Executive need not demonstrate that disclosure of the asserted state secrets *will* impair the defense of the nation, disclose intelligence-gathering capabilities and methods, or disrupt foreign relations. Rather, the Executive need only show a "reasonable danger" that these harms may arise,[44] or a "reasonable possibility that military or state secrets would be revealed."[45] Furthermore, courts must be careful to remember that "intelligence gathering . . . is more akin to the construction of a mosaic than it is to the management of a cloak and dagger affair. Thousands of bits and pieces of seemingly innocuous information can be analyzed and fitted into place to reveal with startling clarity how the unseen whole must operate."[46] And when determining what information is to be protected by the privilege, non-sensitive information should be segregated from protected information to allow for the disclosure of the former.[47] Last, the privilege protects not only the existence of a secret government program but also the method and means of such a program. This is so even where the existence of the secret program has been disclosed.[48]

Judge Taylor and Judge Walker applied these doctrines with mixed results. As to the confirmed "contents" element of the TSP, despite the fact that the Government has disclosed neither the method and means of surveillance nor the intended targets of the surveillance, Judge Taylor—arguably in disregard of *Halkin v. Helms*—concluded that this element of the TSP is not a state secret.[49] Judge Taylor did, however, rule that the alleged records element of the TSP is a state secret and dismissed the records-based claims. Judge Walker similarly concluded that the confirmed contents element of the TSP is not a state secret. In his view, because the Government had already admitted the TSP's existence, along with a few details about the TSP, there could be no danger of divulging sensitive state secrets.[50] Indeed, he permitted discovery as to whether AT&T received a certification from the Government directing AT&T to assist it in monitoring communications content. Interestingly, Judge Walker declined to rule as to the alleged records element of the TSP. Although implying that this element of the TSP is a state secret, Judge Walker emphasized that the Government could make disclosures during litigation that make the subscriber records program "no longer a secret" and so he denied the Government's motion to dismiss.

These decisions yield a less than robust state secrets privilege. First, to the extent the courts failed to protect the contents element of the TSP under the privilege, the courts appeared to ignore the rule that the mere fact of the existence of an otherwise secret government program does not warrant the disclosure of the means and methods of its operation. Second, Judge Walker's decision to allow the claims based on the alleged records element of the TSP to survive seems to flip the state secrets doctrine on its head. It tends to support a regime that favors disclosure, not one in which courts should generally defer to Executive assertions of the privilege. Indeed, Judge Walker's decision appears to assume there is a "reasonable possibility that military or state secrets [about the alleged records element] will be revealed."[51]

These decisions on the state secrets privilege could have far-reaching implications and lead to unintended and harmful results. Principally, they appear to undermine the Government's methods of conducting the war on terror by disclosing the method and means of the contents element of the TSP and the targets of surveillance. They may thus hinder the Government's arms of intelligence procurement.[52] In addition, these decisions would lead to an absurd result with regard to private cooperation in matters of national security. In *Totten v. United States*[53] and *Tenet v. Doe*,[54] the Court emphasized the Government's need and authority to keep secret arrangements secret, holding that parties to contracts with the Government may not sue on those contracts if their subject matter is a state secret. The decisions by Judge Taylor and Judge Walker may diminish cooperation between the Government and American businesses. Their rulings would permit third parties to sue American businesses for their actions in cooperating with the Government and force disclosure of the nature of those cooperative relationships even though American businesses themselves could be prohibited from disclosing these cooperative relationships and possibly from seeking the protection of the Government from any liability arising from their cooperative actions. Such a result would impose incalculable financial risks. Now more than ever, perhaps, it is more important the courts clarify the scope of the state secrets doctrine and decide whether American businesses have a continued role to play in national security.

**Endnotes**

1 James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times, Dec. 16, 2005, at A1.

2 On September 14, 2001, Congress passed a joint resolution, commonly known as the Authorization for the Use of Military Force, that 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 . . . or harbored such organizations or persons." Authorization for Use of Military Force, Pub. L. 107-40, §§ 1-2, 115 Stat. 224 ("AUMF").

3 The White House, President's radio address, *available at* http://www.whitehouse.gov/news/releases/2005/12/print/20051217.html (last visited Jan. 26, 2007). Attorney General Alberto Gonzales subsequently made a similar public statement confirming the existence of and minimally describing the TSP. *See* The White House, Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence (Dec. 19, 2005), *available at* http://www.whitehouse.gov/news/releases/2005/12/print/20051219-1.html (last visited Jan. 26, 2007). Several similar statements were made about the TSP by Executive officials. *See, e.g.*, The White House, *President Bush Discusses NSA Surveillance Program* (May 11, 2006), *available at* http://www.whitehouse.gov/news/releases/2006/05/20060511-1.html (last visited Dec. 10, 2006); U.S. Department of Justice, *Legal Authorities Supporting the Activities of the National Security Agency Described by the President* (Jan. 19, 2006), *available at* http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf. The Bush Administration has neither confirmed nor denied that "purely domestic calls and electronic communications are being monitored." David Kravets, *Judge Mulling Whether to Dismiss Spy Lawsuit*, Associated Press State & Local Wire, June 23, 2006; *see also* Hepting v. AT&T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006).

4 Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA Today, May 11, 2006, A1; *see also* Bruce Landis, *Utilities Chief May Probe Call Screening*, The Providence Journal, July 23, 2006, B-01.

5 *See* News Release, Bellsouth Corporation, *BellSouth Statement on Governmental Data Collection* (May 15, 2006), *available at* http://bellsouth.mediaroom.com/index.php?s=press_releases&item=2860 (last visited Jan. 26, 2007); News Release, Verizon Issues Statement on NSA Media Coverage (May 16, 2006), *available at* http://newscenter.verizon.com/press-releases/verizon/2006/page.jsp?itemID=29670712 (last visited Jan. 26, 2007).

6 Donna Walter, *Missouri Lawsuit Seeks to Stop Phone Inquiry*, Kansas City Daily Record, July 31, 2006, NEWS (reporting that "[s]ince January, more than 30 class action lawsuits have been filed against telecommunications carriers alleging they unlawfully assisted the NSA"). Complaints raising similar issues are also pending before state regulatory commissions. *See, e.g.*, In the Matter of the Complaint of the American Civil Liberties Union Fund of Michigan, et al. against AT&T Michigan and Verizon North, Inc., Mich. Pub. Serv. Comm'n, Case U-14985 (filed July 26, 2006).

7 50 U.S.C. § 1801 *et seq*.

8 18 U.S.C. § 2511

9 18 U.S.C. § 2701 *et seq*.

10 *See* Hepting v. AT&T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006); ACLU v. NSA, 438 F. Supp. 2d 754 (E.D. Mich. 2006).

11 *ACLU,* 438 F. Supp. 2d 754.

12 *See id.* at 758-9.

13 *See id.* at 782. This opinion has been criticized as not being well-reasoned, even by many who agree with the result. *See* Adam Liptak, *Many Experts Fault Reasoning In Surveillance Decision*, N.Y. Times, Aug. 19, 2006, A1 ("Some scholars speculated that Judge Taylor . . . may have rushed her decision lest the case be consolidated with several others now pending in federal court in San Francisco or moved to a specialized court in Washington as contemplated by pending legislation.").

14 *See* ACLU v. NSA, 467 F.3d 590 (6th Cir. 2006). Oral argument was scheduled for January 31, 2007.

15 *Hepting,* 439 F. Supp. 2d at 978-979; *see* David Kravets, *Bush Administration Demanding Spy Lawsuit Dismissal*, Associated Press State & Local Wire, June 23, 2006.

16 Over 30 actions have been consolidated in this MDL in the Northern District of California. *See In re National Security Agency Telecommunications Records Litig.*, M:06-cv-01791-VRW.

17 *See Hepting,* 439 F. Supp. 2d at 979.

18 ACLU compl. ¶ 2, *available at* http://www.aclu.org/images/nsaspying/asset_upload_file137_23491.pdf (last visited Jan. 27, 2006).

19 ACLU v. NSA, 438 F. Supp. 2d 754, 776 (E.D. Mich. 2006).

20 *See* Defendants' Motion to Dismiss or, in the Alternative, for Summary Judgment, *available at* http://cryptome.org/aclu-34.pdf (last visited Dec. 14, 2006).

21 Laird v. Tatum, 408 U.S. 1, 2 (1972).

22 *Id.* at 13-14.

23 It does not appear that plaintiffs have challenged the alleged records element of the TSP on Fourth Amendment grounds. Such an attack would very likely be unsuccessful anyway because telecommunications subscribers have no privacy interest in the records of their communications and thus the acquisition of such records does not constitute a search within the meaning of the Fourth Amendment. *See* Smith v. Maryland, 442 U.S. 735, 744 (1979); United States v. Miller, 425 U.S. 435, 440 (1976); *Reporters Comm. for Freedom of the Press v. AT&T*, 593 F.2d 1030, 1045 (D.C. Cir. 1978).

24 *ACLU,* 438 F. Supp. 2d at 778.

25 *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 266 (1990) ("What we know of the history of the drafting of the Fourth Amendment also suggests that its purpose was to restrict searches and seizures which might be conducted by the United States in domestic matters."); *see id.* at 267 (holding that the Fourth Amendment does not "apply to activities of the United States directed against aliens in foreign territory or in international waters").

26 *See* Johnson v. Eisentrager, 339 U.S. 763, 775 (1950) ("[I]t seems not to have been supposed [by the Founders] that a nation's obligations to its foes could ever be put on parity with those to its defenders."); Kwong Hai Chew v. Colding, 344 U.S. 590, 596 n.5 (1953) ("once an alien *lawfully* enters and resides in this country he becomes invested with the rights guaranteed by the

Constitution to all people within our borders") (emphasis added); United States v. Esparza-Mendoza, 265 F. Supp. 2d 1254, 1271 (D. Utah 2003) (previously deported alien felons lack a "sufficient connection to this country" and thus "stand outside 'the People' covered by the Fourth Amendment").

27 Hepting v. AT&T Corp., 439 F. Supp. 2d 974, 986 (N.D. Cal. 2006)

28 In re Sealed Case, 310 F.3d 717, 742 (Foreign Intel.Surv.Ct.Rev. 2002).

29 *Hepting*, 439 F. Supp 2d at 986.

30 The White House, President's radio address, *available at* http://www.whitehouse.gov/news/releases/2005/12/print/20051217.html (last visited Jan. 26, 2007).

31 *See* United States v. Hall, 488 F.2d 193, 198 (9th Cir. 1973) ("It would be absurd to hold that one is constitutionally protected from any untoward results when he makes statements at a time when he has reason to know some third party is, or probably is, listening.").

32 In enacting FISA, Congress amended the Wiretap Act such that Section 2511(2)(f) now provides that the procedures outlined in FISA, the Wiretap Act and ECPA constitute "the exclusive means by which electronic surveillance … and the interception of domestic wire, oral, and electronic communications may be conducted." 18 U.S.C. § 2511(2)(f).

33 *See* Hepting, 439 F. Supp 2d at 978-79; ACLU v. NSA, 438 F. Supp. 2d 754, 758 (E.D. Mich. 2006). Judge Taylor accepted this argument, noting that "the President has acted, undisputedly, as FISA forbids," and reasoning that his "presidential power, therefore, was exercised at its lowest ebb and cannot be sustained." *ACLU*, 438 F. Supp. 2d at 778.

34 U.S. Const. art II, § 2.

35 Pub. L. 107-40, §§ 1-2, 115 Stat. 224.

36 *See* Tenet v. Doe, 544 U.S. 1 (2005); United States v. Reynolds, 345 U.S. 1 (1953); Totten v. United States, 92 U.S. 105 (1875).

37 *See Hepting*, 439 F. Supp. 2d at 984; Kasza v. Browner, 133 F.3d 1159 (9th Cir. 1998).

38 *See Reynolds*, 345 U.S. at 11 n.26; *Totten*, 92 U.S. at 107.

39 *See Tenet*, 544 U.S. at 9; *Totten*, 92 U.S. at 107.

40 For a more detailed description of the state secrets doctrine, *see* Claudio Ochoa's preceding article in this section.

41 *Totten*, 92 U.S. at 107.

42 Ellsberg v. Mitchell, 709 F.2d 51, 57 (D.C. Cir. 1983) ("No competing public or private interest can be advanced to compel disclosure.").

43 *See* El-Masri v. Tenet, No. 1:05-cv-01417 (E.D. Va. May 12, 2006). *See also* Halkin v. Helms, 598 F.2d 1, 8 (D.C. Cir. 1978).

44 *Ellsberg*, 709 F.2d at 58.

45 Jabara v. Kelley, 75 F. R.D. 475, 484 (E.D. Mich. 1977).

46 *Halkin*, 598 F.2d at 8.

47 *Ellsberg*, 709 F.2d at 57.

48 *See* El-Masri, No. 1:05-cv-01417 (E.D. Va. May 12, 2006).

49 ACLU v. NSA, 438 F. Supp. 2d 754, 778 (E.D. Mich. 2006).

50 Hepting v. AT&T Corp., 439 F. Supp. 2d 974, 991-992 (N.D. Cal. 2006); *see also Administration Appeals Domestic Spying Decision,* Associated Press State & Local Wire, Aug. 1, 2006.

51 Jabara v. Kelley, 75 F. R.D. 475, 484 (E.D. Mich. 1977).

52 This is so even though the President has elected to conduct "electronic surveillance that was occurring as part of the [TSP]" under the approval of the Foreign Intelligence Surveillance Court ("FISA Court") and not to reauthorize the TSP. *See* Letter from Attorney General Alberto R. Gonzales to Sens. Patrick Leahy & Arlen Specter of Jan. 17, 2007. Indeed, despite this decision to conduct pursuant to FISA Court approval electronic surveillance that was formerly a part of the TSP, the Government has continued to highlight the importance of protecting state secrets relating to the TSP. *See* Government's Supp. Submission Discussing the Implications of the Intervening FISA Court Orders of January 10, 2007 at 19-20, *ACLU v. NSA*, Nos. 06-2095, -2140 (6th Cir. filed Jan. 24, 2007).

53 92 U.S. 105 (1875).

54 544 U.S. 1 (2005).